Kaspersky Anti-Virus 6.0 per Windows Workstations MP4

MANUALE DELL'UTENTE

VERSIONE DELL'APPLICAZIONE: 6.0 MAINTENANCE PACK 4

Gentile utente di Kaspersky Anti-Virus,

Grazie per aver scelto il nostro prodotto. Ci auguriamo che questa documentazione sia utile e fornisca le risposte necessarie.

Il presente documento è soggetto a modifica senza preavviso. Per la versione più recente del presente documento, visitare il sito Web di Kaspersky Lab all'indirizzo http://www.kaspersky.com/it/docs.

Data di revisione: 08.09.2009

http://www.kaspersky.it
http://support.kaspersky.it

SOMMARIO

INTRODUZIONE ... 11

Kit di distribuzione ... 11

Contratto di licenza con l'utente finale (EULA) ... 11

Servizi offerti agli utenti registrati ... 11

Requisiti di sistema hardware e software ... 12

KASPERSKY ANTI-VIRUS 6.0 PER WINDOWS WORKSTATIONS MP4 ... 13

Informazioni sull'applicazione ... 13

Fonti di informazione per l'esecuzione di ricerche ... 13

Come contattare l'ufficio vendite ... 14

Come contattare il servizio di assistenza tecnica ... 14

Discussioni sulle applicazioni Kaspersky Lab nel forum Web ... 15

Novità di Kaspersky Anti-Virus 6.0 per Windows Workstations MP4 ... 15

Difesa di Kaspersky Anti-Virus: le basi ... 17

Componenti di protezione ... 17

Attività di scansione anti-virus ... 18

Aggiornamento ... 18

Funzioni di assistenza dell'applicazione ... 18

INSTALLAZIONE DI KASPERSKY ANTI-VIRUS 6.0 ... 20

Installazione tramite procedura guidata ... 20

Passaggio 1. Verifica dei requisiti di installazione del sistema ... 21

Passaggio 2. Finestra di avvio dell'installazione ... 21

Passaggio 3. Visualizzazione del Contratto di licenza ... 21

Passaggio 4. Selezione della cartella di installazione ... 21

Passaggio 5. Utilizzo delle impostazioni dell'applicazione salvate dopo un'installazione precedente ... 22

Passaggio 6. Selezione del tipo di installazione ... 22

Passaggio 7. Selezione dei componenti dell'applicazione per l'installazione ... 22

Passaggio 8. Disabilitazione del firewall di Microsoft Windows ... 23

Passaggio 9. Ricerca di altre applicazioni anti-virus ... 23

Passaggio 10. Preparazione finale per l'installazione ... 23

Passaggio 11. Completamento dell'installazione ... 24

Installazione dell'applicazione da riga di comando ... 24

Installazione dall'editor Oggetti criteri di gruppo ... 24

Installazione dell'applicazione ... 25

Descrizione delle impostazioni del file setup.ini ... 25

Aggiornamento della versione dell'applicazione ... 26

Rimozione dell'applicazione ... 26

OPERAZIONI PRELIMINARI ... 27

Configurazione guidata iniziale ... 28

Utilizzo degli oggetti salvati dalla versione precedente ... 28

Attivazione dell'applicazione ... 28

Modalità di protezione ... 30

Configurazione delle impostazioni di aggiornamento ... 30

Configurazione della pianificazione della scansione anti-virus ... 31

Limitazione dell'accesso all'applicazione ... 31

Configurazione di Anti-Hacker ... 32
Completamento della configurazione guidata ... 34
Scansione anti-virus del computer ... 34
Aggiornamento dell'applicazione ... 34
Gestione delle licenze ... 35
Gestione della protezione ... 35
Sospensione della protezione ... 36
Eliminazione dei problemi. Assistenza tecnica utente ... 37
Creazione di un file di traccia ... 37
Configurazione delle impostazioni dell'applicazione ... 38
Rapporti sul funzionamento dell'applicazione. File di dati ... 38
INTERFACCIA DELL'APPLICAZIONE ... 39
Icona dell'area di notifica della barra delle applicazioni ... 39
Menu di scelta rapida ... 40
Finestra principale dell'applicazione ... 41
Notifiche ... 43
Finestra delle impostazioni dell'applicazione ... 44
ANTI-VIRUS FILE ... 45
Algoritmo di funzionamento del componente ... 46
Modifica del livello di protezione ... 47
Modifica delle azioni da eseguire sugli oggetti rilevati ... 48
Creazione di un ambito di protezione ... 49
Utilizzo dell'analisi euristica ... 50
Ottimizzazione della scansione ... 50
Scansione dei file compositi ... 51
Scansione di file composti di grandi dimensioni ... 51
Modifica della modalità di scansione ... 52
Tecnologia di scansione ... 52
Sospensione del componente: creazione di una pianificazione ... 53
Sospensione del componente: creazione di un elenco di applicazioni ... 53
Ripristino delle impostazioni di protezione predefinite ... 54
Statistiche di Anti-Virus File ... 54
Trattamento posticipato degli oggetti ... 55
ANTI-VIRUS POSTA ... 56
Algoritmo di funzionamento del componente ... 57
Modifica del livello di protezione ... 58
Modifica delle azioni da eseguire sugli oggetti rilevati ... 59
Creazione di un ambito di protezione ... 60
Selezione del metodo di scansione ... 60
Scansione della posta elettronica in Microsoft Office Outlook ... 61
Scansione della posta elettronica nel plug-in The Bat! ... 62
Utilizzo dell'analisi euristica ... 62
Scansione dei file compositi ... 63
Filtro degli allegati ... 63
Ripristino delle impostazioni di protezione della posta elettronica predefinite ... 64
Statistiche della protezione della posta elettronica ... 64

ANTI-VIRUS WEB ... 66
Algoritmo di funzionamento del componente ... 67
Modifica del livello di protezione del traffico HTTP ... 68
Modifica delle azioni da eseguire sugli oggetti rilevati ... 68
Creazione di un ambito di protezione ... 69
Selezione del metodo di scansione ... 69
Utilizzo dell'analisi euristica ... 70
Ottimizzazione della scansione ... 70
Ripristino delle impostazioni di protezione Web predefinite ... 71
Statistiche di Anti-Virus Web ... 71
DIFESA PROATTIVA ... 73
Algoritmo di funzionamento del componente ... 74
Analisi attività applicazione ... 74
Utilizzo dell'elenco di attività pericolose ... 75
Modifica delle regole per il monitoraggio delle attività pericolose ... 75
Controllo degli account di sistema ... 76
Eventi di Difesa Proattiva ... 76
Registry Guard ... 79
Gestione dell'elenco di regole di monitoraggio del registro di sistema ... 79
Creazione di un gruppo di elementi del registro di sistema da monitorare ... 80
Statistiche di Difesa Proattiva ... 82
ANTI-SPY ... 83
Anti-Banner ... 83
Creazione dell'elenco di indirizzi di banner consentiti ... 84
Creazione dell'elenco di indirizzi di banner bloccati ... 84
Impostazioni avanzate del componente ... 84
Esportazione / importazione degli elenchi di banner ... 85
Anti-Dialer ... 86
Statistiche di Anti-Spy ... 86
PROTEZIONE DAGLI ATTACCHI DI RETE ... 87
Schema di funzionamento del componente ... 88
Modifica del livello di protezione di Anti-Hacker ... 89
Regole per applicazioni e filtraggio pacchetti ... 90
Regole per le applicazioni. Creazione manuale di una regola ... 90
Regole per le applicazioni. Creazione di regole con modelli ... 91
Regole per i filtri pacchetti. Creazione di una regola ... 92
Modifica della priorità di una regola ... 92
Esportazione e importazione delle regole create ... 93
Ottimizzazione delle regole per applicazioni e filtraggio pacchetti ... 93
Regole per zone di sicurezza ... 96
Aggiunta di nuove zone di sicurezza ... 97
Modifica dello stato di una zona di sicurezza ... 98
Abilitazione / disabilitazione della modalità Mascheramento ... 98
Modifica della modalità Firewall ... 98
Sistema di rilevamento intrusioni ... 99
Monitor di rete ... 100
Tipi di attacchi di rete ... 100
Statistiche di Anti-Hacker ... 102

ANTI-SPAM ... 103
Algoritmo di funzionamento del componente ... 104
Addestramento di Anti-Spam ... 106
Addestramento con Apprendimento guidato ... 106
Addestramento tramite i messaggi di posta elettronica in uscita ... 107
Addestramento tramite il client di posta ... 107
Addestramento con i rapporti ... 108
Modifica del livello di sensibilità ... 109
Filtro dei messaggi di posta sul server. Gestore della posta ... 109
Esclusione di messaggi di Microsoft Exchange Server dalla scansione ... 110
Selezione del metodo di scansione ... 111
Selezione della tecnologia di filtro anti-spam ... 111
Determinazione dei fattori di spam e probabile spam ... 112
Utilizzo delle funzioni avanzate di filtro anti-spam ... 112
Creazione dell'elenco di mittenti consentiti ... 113
Creazione dell'elenco di frasi consentite ... 114
Importazione dell'elenco di mittenti consentiti ... 114
Creazione dell'elenco di mittenti bloccati ... 115
Creazione dell'elenco di frasi bloccate ... 116
Azioni da eseguire con la posta spam ... 116
Configurazione dell'elaborazione della posta spam in Microsoft Office Outlook ... 117
Configurazione dell'elaborazione della posta spam in Microsoft Outlook Express (Windows Mail) ... 118
Configurazione dell'elaborazione della posta spam in The Bat! ... 119
Ripristino delle impostazioni predefinite di Anti-Spam ... 120
Statistiche Anti-Spam ... 120

CONTROLLO ACCESSI ... 122
Controllo dispositivo. Limitazione dell'utilizzo di dispositivi esterni ... 122
Controllo dispositivo. Disabilita autorun ... 123
Statistiche di Controllo Accessi ... 123

SCANSIONE ANTI-VIRUS DEL COMPUTER ... 124
Avvio della scansione anti-virus ... 125
Creazione di un elenco di oggetti da esaminare ... 126
Modifica del livello di protezione ... 127
Modifica delle azioni da eseguire sugli oggetti rilevati ... 127
Modifica del tipo di oggetti da esaminare ... 129
Ottimizzazione della scansione ... 129
Scansione dei file compositi ... 130
Tecnologia di scansione ... 130
Modifica del metodo di scansione ... 131
Prestazioni del computer durante l'esecuzione delle attività ... 131
Modalità di esecuzione: specifica di un account ... 132
Modalità di esecuzione: creazione di una pianificazione ... 132
Funzioni dell'avvio pianificato delle attività ... 133
Statistiche della scansione anti-virus ... 133
Assegnazione delle impostazioni di scansione comuni per tutte le attività ... 134
Ripristino delle impostazioni di scansione predefinite ... 134

AGGIORNAMENTO DELL'APPLICAZIONE ... 135
Avvio dell'aggiornamento ... 136

Rollback dell'ultimo aggiornamento ... 137
Origine degli aggiornamenti ... 137
Impostazioni internazionali ... 138
Utilizzo di un server proxy ... 138
Modalità di esecuzione: specifica di un account ... 139
Modalità di esecuzione: creazione di una pianificazione ... 139
Modifica della modalità di esecuzione dell'attività di aggiornamento ... 140
Selezione degli oggetti da aggiornare ... 141
Aggiornamento da una cartella locale ... 141
Statistiche di aggiornamento ... 142
Problemi possibili durante l'aggiornamento ... 142
CONFIGURAZIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE ... 147
Protezione ... 149
Abilitazione / disabilitazione della protezione del computer ... 150
Avvio dell'applicazione all'avvio del sistema operativo ... 150
Utilizzo della tecnologia avanzata di disinfezione ... 150
Selezione delle categorie di minacce rilevabili ... 151
Creazione di un'area attendibile ... 151
Esportazione/importazione delle impostazioni di Kaspersky Anti-Virus ... 155
Ripristino delle impostazioni predefinite ... 156
Anti-Virus File ... 157
Anti-Virus Posta ... 157
Anti-Virus Web ... 158
Difesa Proattiva ... 159
Anti-Spy ... 159
Anti-Hacker ... 160
Anti-Spam ... 161
Scansione ... 162
Aggiornamento ... 163
Opzioni ... 163
Auto-difesa dell'applicazione ... 164
Limitazione dell'accesso all'applicazione ... 164
Utilizzo dell'applicazione su un laptop ... 165
Limitazione delle dimensioni dei file iSwift ... 165
Notifiche degli eventi di Kaspersky Anti-Virus ... 165
Elementi attivi dell'interfaccia ... 167
Rapporti e archiviazioni ... 168
Principi di gestione dei rapporti ... 169
Configurazione dei rapporti ... 169
Quarantena per oggetti potenzialmente infetti ... 170
Azioni sugli oggetti in quarantena ... 170
Copie di backup degli oggetti pericolosi ... 171
Utilizzo delle copie di backup ... 171
Configurazione della quarantena e del backup ... 171
Rete ... 172
Creazione di un elenco di porte da monitorare ... 172
Scansione delle connessioni crittografate ... 173
Scansione delle connessioni crittografate in Mozilla Firefox ... 174

Scansione delle connessioni crittografate in Opera ... 174

DISCO DI RIPRISTINO ... 176

Creazione del Disco di Ripristino ... 176

Passaggio 1. Selezione dell'origine dell'immagine del Disco di emergenza ... 177

Passaggio 2. Copia dell'immagine ISO ... 177

Passaggio 3. Aggiornamento dell'immagine ISO ... 177

Passaggio 4. Avvio remoto ... 178

Passaggio 5. Chiusura della procedura guidata ... 178

Avvio del computer attraverso il Disco di Ripristino ... 178

Utilizzo del Disco di Ripristino di Kaspersky dal prompt dei comandi ... 181

Scansione anti-virus ... 181

Aggiornamento di Kaspersky Anti-Virus ... 183

Rollback dell'ultimo aggiornamento ... 183

Visualizzazione della Guida ... 184

VERIFICA DEL FUNZIONAMENTO DI KASPERSKY ANTI-VIRUS ... 185

"Virus" di prova EICAR e sue varianti ... 185

Test della protezione del traffico HTTP ... 186

Test della protezione del traffico SMTP ... 187

Verifica del funzionamento di Anti-Virus File ... 187

Verifica del funzionamento dell'attività di scansione anti-virus ... 187

Verifica del funzionamento di Anti-Spam ... 188

TIPI DI NOTIFICHE ... 189

Rilevamento di un oggetto dannoso ... 189

Impossibile disinfettare l'oggetto ... 190

Richiesta di esecuzione di una procedura speciale ... 191

Rilevamento di un oggetto sospetto ... 191

Rilevamento di un oggetto pericoloso nel traffico ... 192

Rilevamento di un'attività pericolosa nel sistema ... 192

Rilevamento di un intruso ... 193

Rilevamento di processi nascosti ... 193

Rilevamento di un tentativo di accesso al Registro di sistema ... 194

Rilevamento di un tentativo di reindirizzamento delle chiamate alle funzioni di sistema ... 194

Rilevamento dell'attività di rete di un'applicazione ... 195

Rilevamento dell'attività di rete di un file eseguibile modificato ... 196

Rilevamento di una nuova rete ... 196

Rilevamento di un attacco di phishing ... 196

Rilevamento di un tentativo di composizione automatica ... 197

Rilevamento di un certificato non valido ... 197

UTILIZZO DELL'APPLICAZIONE DALLA RIGA DI COMANDO ... 198

Visualizzazione della Guida ... 199

Scansione anti-virus ... 199

Aggiornamento dell'applicazione ... 201

Rollback dell'ultimo aggiornamento ... 202

Avvio/arresto di un componente di protezione o di un'attività ... 202

Statistiche sul funzionamento di un componente o di un'attività ... 204

Esportazione delle impostazioni di protezione ... 204

Importazione delle impostazioni di protezione ... 204

Attivazione dell'applicazione 205
Ripristino di un file dalla quarantena 205
Chiusura dell'applicazione 205
Come ottenere un file di chiave 206
Codici restituiti della riga di comando 206
MODIFICA, RIPARAZIONE E RIMOZIONE DELL'APPLICAZIONE 207
Modifica, riparazione e rimozione dell'applicazione tramite l'installazione guidata 207
Passaggio 1. Finestra iniziale dell'installazione 207
Passaggio 2. Selezione di un'operazione 208
Passaggio 3. Completamento della modifica, riparazione o rimozione dell'applicazione 208
Rimozione dell'applicazione dalla riga di comando 209
GESTIONE DELL'APPLICAZIONE TRAMITE KASPERSKY ADMINISTRATION KIT 210
Gestione dell'applicazione 212
Avvio e arresto dell'applicazione 213
Configurazione delle impostazioni dell'applicazione 215
Configurazione di impostazioni specifiche 217
Gestione delle attività 218
Avvio e arresto delle attività 219
Creazione di attività 220
Creazione guidata attività locale 221
Configurazione delle attività 222
Gestione dei criteri 224
Creazione di criteri 224
Creazione guidata criterio 225
Configurazione del criterio 227
UTILIZZO DI CODICE DI TERZE PARTI 229
Libreria Boost 1.30 230
Libreria LZMA SDK 4.40, 4.43 230
Libreria Windows Template (WTL 7.5) 230
Libreria Windows Installer XML (WiX-2.0) 231
Libreria ZIP-2.31 234
Libreria ZLIB-1.0.4, ZLIB-1.1.3, ZLIB-1.2.3 235
Libreria UNZIP-5.51 235
Libreria LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12 236
Libreria LIBJPEG-6B 238
Libreria LIBUNGIF-4.1.4 239
Libreria MD5 MESSAGE-DIGEST ALGORITHM-REV. 2 239
Libreria MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004 239
Libreria INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999 240
Libreria CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004 240
Libreria COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum 240
Libreria PLATFORM INDEPENDENT IMAGE CLASS 241
Libreria FLEX PARSER (FLEXLEXER)-V. 1993 241
Libreria ENSURECLEANUP, SWMRG, LAYOUT-V. 2000 241
Libreria STDSTRING- V. 1999 242
Libreria T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006 242
Libreria NTSERVICE- V. 1997 243
Libreria SHA-1-1.2 243

INTRODUZIONE

IN QUESTA SEZIONE

Kit di distribuzione 11

Servizi offerti agli utenti registrati 11

Requisiti di sistema hardware e software 12

KIT DI DISTRIBUZIONE

Kaspersky Anti-Virus può essere acquistato presso i nostri rivenditori oppure online dai negozi su Internet, ad esempio nella sezione **Compra Online** del sito http://www.kaspersky.it.

Il pacchetto della versione in scatola del prodotto include:

- Una busta sigillata con il CD di installazione contenente i file del programma e la documentazione in formato PDF.
- La Guida dell'utente stampata (se è stata inclusa nell'ordine) oppure la Guida del prodotto.
- File di chiave dell'applicazione allegato alla busta del CD di installazione.
- Scheda di registrazione (con numero di serie del prodotto).
- Contratto di licenza con l'utente finale (EULA).

Si consiglia di leggere attentamente le condizioni dell'EULA prima di aprire la busta del CD di installazione.

L'acquisto di Kaspersky Anti-Virus presso il negozio online comporta il download del prodotto dal sito Web di Kaspersky Lab. Il presente Manuale dell'utente è incluso nel pacchetto di installazione. Alla ricezione del pagamento, l'utente riceverà un messaggio di posta elettronica con il file di chiave.

CONTRATTO DI LICENZA CON L'UTENTE FINALE (EULA)

Il Contratto di licenza con l'utente finale (EULA) è un contratto legale che intercorre tra l'utente e Kaspersky Lab, in cui si specificano le condizioni di utilizzo del software acquistato.

L'EULA deve essere letto con molta attenzione.

Se non si accettano le condizioni dell'EULA, è possibile restituire la confezione del prodotto al rivenditore presso il quale è stata acquistata e ottenere il rimborso corrispondente all'importo pagato, a condizione che la busta contenente il disco di installazione sia ancora sigillata.

L'apertura della busta sigillata con il CD di installazione implica l'accettazione delle condizioni dell'EULA.

SERVIZI OFFERTI AGLI UTENTI REGISTRATI

Kaspersky Lab offre un pacchetto completo di servizi a tutti gli utenti legalmente registrati, consentendo loro di potenziare le prestazioni dell'applicazione.

Con l'acquisto di una licenza si diventa utente registrato e si può usufruire durante tutto il periodo di durata della licenza dei servizi seguenti:

- aggiornamenti orari dei database dell'applicazione e aggiornamento al pacchetto software;
- supporto per i problemi correlati all'installazione, alla configurazione e all'utilizzo del prodotto software acquistato. I servizi vengono forniti tramite telefono o posta elettronica;
- notifiche relative ai nuovi prodotti Kaspersky Lab e ai nuovi virus che si diffondono in tutto il mondo. Questo servizio è disponibile per gli utenti che hanno effettuato la sottoscrizione alla mailing list delle news di Kaspersky Lab nelsito Web del servizio di assistenza tecnica (http://support.kaspersky.com/it/subscribe/).

Non viene fornito supporto per i problemi correlati alle prestazioni e all'utilizzo dei sistemi operativi, altro software di terzi o altre tecnologie.

REQUISITI DI SISTEMA HARDWARE E SOFTWARE

Per il corretto funzionamento di Kaspersky Anti-Virus 6.0, il computer deve soddisfare i requisiti minimi seguenti:

Requisiti generali:

- 300 MB di spazio libero su disco rigido.
- Microsoft Internet Explorer 6.0 o versione successiva (per l'aggiornamento dei database dell'applicazione e dei moduli del programma via Internet).
- Microsoft Windows Installer 2.0 o superiore.

Microsoft Windows 2000 Professional (Service Pack 4 Rollup1), Microsoft Windows XP Professional (Service Pack 2 o superiore), Microsoft Windows XP Professional x64 (Service Pack 2 o superiore):

- Processore Intel Pentium da 300 MHz 32 bit (x86) / 64 bit (x64) o superiore (o un processore equivalente compatibile).
- 256 MB di RAM libera.

Microsoft Windows Vista Business / Enterprise / Ultimate (Service Pack 1 o superiore), Microsoft Windows Vista Business / Enterprise / Ultimate x64 (Service Pack 1 o superiore), Microsoft Windows 7 Professional / Enterprise / Ultimate, Microsoft Windows 7 Professional / Enterprise / Ultimate x64:

- Processore Intel Pentium da 800 MHz 32 bit (x86) / 64 bit (x64) o superiore (o un processore equivalente compatibile).
- 512 MB di RAM libera.

KASPERSKY ANTI-VIRUS 6.0 PER WINDOWS WORKSTATIONS MP4

Kaspersky Anti-Virus 6.0 per Windows Workstations MP4 annuncia una nuova generazione di prodotti per la sicurezza dei dati.

Ciò che distingue Kaspersky Anti-Virus 6.0 per Windows Workstations da tutti gli altri software, persino dagli altri prodotti Kaspersky Lab, è la completezza della protezione dei dati del computer dell'utente.

IN QUESTA SEZIONE

Informazioni sull'applicazione 13

Novità di Kaspersky Anti-Virus 6.0 per Windows Workstations MP4 15

Difesa di Kaspersky Anti-Virus: le basi 17

INFORMAZIONI SULL'APPLICAZIONE

Per tutte le domande relative all'acquisto, all'installazione o all'utilizzo di Kaspersky Anti-Virus sono state predisposte le risposte più appropriate.

Kaspersky Lab offre diverse fonti di informazioni sull'applicazione. È possibile scegliere la più adatta in base all'urgenza e all'importanza del quesito.

IN QUESTA SEZIONE

Fonti di informazione per l'esecuzione di ricerche 13

Come contattare l'ufficio vendite 14

Come contattare il servizio di assistenza tecnica 14

Discussioni sulle applicazioni Kaspersky Lab nel forum Web 15

FONTI DI INFORMAZIONE PER L'ESECUZIONE DI RICERCHE

È possibile fare riferimento alle fonti di informazioni sull'applicazione seguenti:

- pagina dell'applicazione nel sito Web di Kaspersky Lab;
- pagina dell'applicazione nel sito Web del servizio di assistenza tecnica (nella Knowledge Base);
- guida in linea;
- documentazione.

Pagina dell'applicazione nel sito Web di Kaspersky Lab

http://www.kaspersky.com/it/anti-virus_windows_workstation

In questa pagina vengono fornite informazioni generali sull'applicazione, nonché sulle relative funzioni e opzioni.

Pagina dell'applicazione nel sito Web del servizio di assistenza tecnica (nella Knowledge Base)

http://support.kaspersky.com/wks

In questa pagina sono presenti articoli creati dagli esperti del servizio di assistenza tecnica.

Tali articoli contengono informazioni utili, consigli e FAQ sull'acquisto, sull'installazione e sull'utilizzo dell'applicazione. Sono organizzati in base all'argomento, ad esempio gestione dei file chiave, impostazione degli aggiornamenti dei database o eliminazione degli errori di funzionamento. Gli articoli possono fornire risposte a domande relative non solo all'applicazione specifica, ma anche ad altri prodotti di Kaspersky Lab. Possono inoltre contenere notizie fornite dal servizio di assistenza tecnica.

Guida in linea

Il pacchetto di installazione dell'applicazione include il file della Guida sensibile al contesto e della Guida completa contenente informazioni sulla modalità di gestione della protezione del computer (visualizzazione dello stato di protezione, scansione anti-virus di diverse aree del computer, esecuzione di altre attività), nonché informazioni su ogni finestra dell'applicazione, quali l'elenco delle relative impostazioni con descrizione associata e l'elenco delle attività da eseguire.

Per aprire il file della Guida, fare clic sul pulsante **Guida** nella finestra desiderata o premere **<F1>**.

Documentazione

Il pacchetto di installazione di Kaspersky Anti-Virus include il documento **Manuale dell'utente** (in formato PDF). Questo documento contiene descrizioni delle funzioni e delle opzioni dell'applicazione, nonché dei principali algoritmi di funzionamento.

COME CONTATTARE L'UFFICIO VENDITE

In caso di domande riguardanti la selezione o l'acquisto dell'applicazione o l'estensione del periodo di utilizzo, è possibile telefonare agli specialisti dell'ufficio vendite nella Sede centrale di Mosca, ai numeri:

+7 (495) 797-87-00, **+7 (495) 645-79-39**, **+7 (495) 956-70-00**

Il servizio è disponibile in russo o in inglese.

È possibile inviare le proprie domande via e-mail all'ufficio vendite all'indirizzo: sales@kaspersky.com.

COME CONTATTARE IL SERVIZIO DI ASSISTENZA TECNICA

Una volta acquistato Kaspersky Anti-Virus, è possibile ottenere tutte le informazioni desiderate dal servizio di assistenza tecnica telefonicamente o tramite Internet.

Gli specialisti del servizio di assistenza tecnica saranno lieti di rispondere a qualsiasi domanda relativa all'installazione e all'utilizzo dell'applicazione. e forniranno consigli preziosi per risolvere i problemi causati dalle attività del malware qualora il computer sia stato infettato.

Prima di contattare il servizio di assistenza tecnica, leggere la sezioneTermini e condizioni dell'assistenza tecnica (http://support.kaspersky.com/it/support/rules).

Richiesta al servizio di assistenza tecnica via posta elettronica

Per inviare le domande agli specialisti del servizio di assistenza tecnica, compilare il modulo Web Helpdesk (http://support.kaspersky.com/helpdesk.html?LANG=it).

La domanda può essere formulata in Italiano, Russo, Inglese, Tedesco, Francese o Spagnolo.

Per inviare una richiesta via e-mail, è necessario indicare l'**ID cliente** ricevuto durante la registrazione al sito Web del servizio di assistenza tecnica insieme alla **password**.

Se non si è ancora un utente registrato delle applicazioni di Kaspersky Lab, è possibile compilare il modulo di registrazione all'indirizzo https://support.kaspersky.com/it/personalcabinet/registration/form/. Durante la registrazione, sarà necessario immettere il *codice di attivazione* o il *nome del file di chiave della licenza*.

La risposta del servizio di assistenza tecnica alla richiesta sarà inviata all'account Kaspersky dell'utente (https://support.kaspersky.com/en/personalcabinet?LANG=it) e all'indirizzo e-mail specificato nella richiesta.

Descrivere il più dettagliatamente possibile il problema riscontrato nel modulo di richiesta Web. Compilare i seguenti campi obbligatori:

- **Tipo di richiesta**. Selezionare l'argomento che si avvicina di più al problema, ad esempio: problema con l'installazione o la disinstallazione oppure problema con la ricerca o l'eliminazione di virus. Se l'argomento desiderato non è disponibile, selezionare "Domanda di carattere generale".
- **Nome e numero di versione dell'applicazione**.
- **Tipo di richiesta**. Descrivere il problema rilevato il più dettagliatamente possibile.
- **ID cliente e password**. Specificare il numero cliente e la password ricevuti durante la registrazione nel sito Web del servizio di assistenza tecnica.
- **Indirizzo e-mail**. Il servizio di assistenza tecnica invierà una risposta alle domande formulate all'indirizzo specificato.

Assistenza tecnica telefonica

Per sottoporre un problema urgente, è possibile contattare telefonicamente il servizio di assistenza tecnica locale. Prima di contattare gli specialisti del servizio di assistenza tecnica russo (http://support.kaspersky.ru/support/support_local) o internazionale (http://support.kaspersky.com/it/support/international) raccogliere le informazioni (http://support.kaspersky.com/it/support/details) sul computer e sull'applicazione anti-virus installata. Ciò consentirà agli esperti di fornire assistenza più rapidamente.

DISCUSSIONI SULLE APPLICAZIONI KASPERSKY LAB NEL FORUM WEB

Se la propria domanda non richiede una risposta urgente, è possibile discuterne con gli specialisti di Kaspersky Lab e altri utenti nel nostro forum all'indirizzo http://forum.kaspersky.com.

In questo forum è possibile visualizzare gli argomenti esistenti, lasciare commenti, creare nuovi argomenti e utilizzare il motore di ricerca.

NOVITÀ DI KASPERSKY ANTI-VIRUS 6.0 PER WINDOWS WORKSTATIONS MP4

Kaspersky Anti-Virus 6.0 è uno strumento completo di protezione dei dati. L'applicazione garantisce non solo la protezione anti-virus ma anche la protezione dagli attacchi spam e di rete. Inoltre, i componenti dell'applicazione consentono agli utenti di proteggere i loro computer da minacce sconosciute e da phishing, nonché limitare l'accesso degli utenti alla rete Internet.

Questa forma di protezione copre tutti i canali di scambio e trasferimento dati. La configurazione flessibile, disponibile per qualsiasi componente, consente agli utenti di adattare con efficacia Kaspersky Anti-Virus alle proprie specifiche esigenze.

Di seguito vengono descritte in modo dettagliato le nuove funzionalità di Kaspersky Anti-Virus 6.0.

Nuova protezione:

- Il nuovo kernel anti-virus utilizzato da Kaspersky Anti-Virus rileva i programmi dannosi in maniera più efficace. Inoltre, consente una scansione anti-virus del sistema molto più rapida. È il risultato di una elaborazione degli oggetti migliorata e di un utilizzo ottimizzato delle risorse del computer (in particolare per i processori dual o quad core).
- È stata implementata una nuova analisi euristica, che fornisce maggiore accuratezza nel rilevamento e nel blocco di programmi dannosi sconosciuti in precedenza. Se la firma di un programma non viene trovata nei database dell'anti-virus, l'analisi euristica simula l'avvio del programma in un ambiente virtuale isolato. Si tratta di un metodo protetto che consente l'analisi di tutti gli effetti di un programma prima del suo avvio in un ambiente reale.
- Il nuovo componente Controllo Accessi esegue il monitoraggio dell'accesso degli utenti a dispositivi I/O, consentendo agli amministratori di limitare l'accesso a unità USB esterne, dispositivi multimedia e altri dispositivi di archiviazione dei dati.
- Sono stati apportati miglioramenti significativi al componente Firewall (è stata migliorata l'efficacia globale di questo componente e aggiunto il supporto IPv6) e alla Difesa Proattiva (è stato ampliato l'elenco degli eventi elaborati dal componente).
- È stata migliorata la procedura di aggiornamento dell'applicazione. Adesso, non è più sempre necessario riavviare il computer.
- È stata aggiunta la funzionalità di scansione del traffico ICQ e MSN, che consente un utilizzo protetto dei client IM.

Funzioni della nuova interfaccia:

- L'interfaccia rende le funzioni del programma di semplice e facile accesso.
- È stata ridisegnata in base alle esigenze degli amministratori di reti piccole e medie, nonché di reti di grandi aziende.

Nuove funzioni di Kaspersky Administration Kit:

- Kaspersky Administration Kit agevola la gestione di un sistema di protezione anti-virus aziendale. Gli amministratori possono utilizzare l'applicazione per gestire in maniera centralizzata la protezione di una rete aziendale di qualsiasi dimensione, contenente decine di migliaia di nodi, inclusi utenti remoti e mobili.
- È stata aggiunta una funzione che abilita l'installazione remota dell'applicazione con la versione più recente dei database dell'applicazione.
- È stata migliorata la gestione dell'applicazione installata su un computer remoto (è stata ridisegnata la struttura dei criteri).
- Ora è possibile gestire da remoto i componenti Anti-Spam e Anti-Spy.
- È stata aggiunta una funzione che consente di utilizzare la configurazione di un'applicazione esistente durante la creazione di un criterio.
- È stata realizzata un'altra funzione importante che consente per gli utenti mobili di creare configurazioni specifiche per la configurazione delle attività di aggiornamento dei gruppi.
- È inoltre stata implementata una funzione per la disabilitazione temporanea delle azioni relative ai criteri e delle attività dei gruppi per i computer client in cui è installata l'applicazione (dopo l'immissione della password corretta).

DIFESA DI KASPERSKY ANTI-VIRUS: LE BASI

La protezione di Kaspersky Anti-Virus è stata costruita tenendo presenti le fonti delle minacce. In altre parole, ogni minaccia viene trattata mediante un componente separato dell'applicazione che la monitora e prende le misure necessarie per prevenire gli effetti dannosi della fonte sui dati dell'utente. Ciò fa dell'impostazione un processo flessibile, offrendo facili opzioni di configurazione per tutti i componenti in modo da soddisfare le esigenze di utenti specifici o di intere aziende.

Kaspersky Anti-Virus include:

- Componenti di protezione (a pag. 17) che proteggono tutti i canali di trasmissione e scambio di dati sul computer in modalità tempo reale.
- Attività Scansione virus (a pag.18) mediante le quali è possibile eseguire scansioni anti-virus del computer o di file, dischi o aree separate.
- Aggiornamento (a pag. 18) garantisce che i moduli interni e i database dell'applicazione, utilizzati per rilevare programmi dannosi, attacchi di rete e messaggi spam, siano aggiornati.
- Funzioni di assistenza (vedere la sezione "Funzioni di assistenza dell'applicazione" a pag. 18) forniscono supporto informativo per l'utilizzo dell'applicazione e l'espansione delle relative funzionalità.

COMPONENTI DI PROTEZIONE

I componenti di protezione seguenti offrono una difesa al computer in tempo reale:

Anti-Virus File (vedere pagina 45)

Anti-Virus File monitora il file system del computer. Esegue la scansione di tutti i file che possono essere aperti, eseguiti o salvati nel computer e di tutte le unità disco connesse. Kaspersky Anti-Virus intercetta ogni tentativo di accedere a un file e ne esegue la scansione allo scopo di individuare virus noti. Il file può essere ulteriormente elaborato solo se non è infetto o se non determina errori nell'applicazione. Se per qualsiasi motivo un file non può essere disinfettato, verrà eliminato e ne verrà salvata una copia nel backup oppure verrà spostato in quarantena.

Anti-Virus Posta (vedere pagina 56)

Anti-Virus Posta esamina tutti i messaggi di posta elettronica in arrivo e in uscita del computer. Analizza i messaggi di posta elettronica alla ricerca di programmi dannosi. Il messaggio di posta elettronica è disponibile per il destinatario solo se non contiene oggetti pericolosi. Il componente inoltre analizza i messaggi di posta elettronica per rilevare phishing.

Anti-Virus Web (vedere pagina 66)

Anti-Virus Web intercetta e blocca gli script nei siti web se costituiscono una minaccia. Tutto il traffico HTTP è sottoposto a un attento esame. Il componente inoltre analizza le pagine Web per rilevare phishing.

Difesa Proattiva (vedere pagina 73)

Difesa Proattiva consente di rilevare un nuovo programma dannoso prima che esegua la propria attività. Il componente è stato progettato per il monitoraggio e l'analisi del comportamento di tutte le applicazioni installate nel computer. Kaspersky Anti-Virus identifica la potenziale pericolosità di un'applicazione in base alle azioni da essa eseguite. Il computer è pertanto protetto non solo dai virus noti ma anche da quelli nuovi, nonché da quelli che non sono stati ancora scoperti.

Anti-Spy (vedere pagina 83)

Anti-Spy controlla gli annunci pubblicitari non autorizzati (banner pubblicitari, finestre popup), intercetta i dialer che tentano di stabilire una connessione con siti Web a pagamento e li blocca.

Anti-Hacker (vedere pagina 87)

Anti-Hacker protegge il computer mentre si naviga in Internet e altre reti. Controlla le connessioni in ingresso e in uscita ed esegue la scansione delle porte e dei pacchetti di dati.

Anti-Spam (vedere pagina 103)

Anti-Spam si integra nel client di posta installato nel computer e monitora tutti i messaggi di posta elettronica in entrata alla ricerca di spam. Tutti i messaggi contenenti spam vengono contrassegnati con un'intestazione speciale. È inoltre possibile configurare Anti-Spam per l'elaborazione dello spam (eliminazione automatica, spostamento in una cartella speciale e così via). Il componente inoltre analizza i messaggi di posta elettronica per rilevare phishing.

Controllo dispositivo (vedere pagina 122)

Il componente è progettato per monitorare l'accesso degli utenti ai dispositivi esterni installati sul computer. Limita l'accesso dell'applicazione a dispositivi esterni (USB, Firewire, Bluetooth e così via).

ATTIVITÀ DI SCANSIONE ANTI-VIRUS

È estremamente importante eseguire la scansione anti-virus periodica del computer. Questa pratica è necessaria per eliminare la possibilità che si diffondano programmi dannosi non rilevati dai componenti di protezione, ad esempio, perché è stato impostato un livello di protezione basso per altri motivi.

In Kaspersky Anti-Virus sono incluse le attività di scansione anti-virus seguenti:

Scansione

Esame degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi oggetto nel file system del computer.

Scansione completa

Scansione approfondita dell'intero sistema. Gli oggetti seguenti vengono esaminati per impostazione predefinita: memoria di sistema, programmi caricati all'avvio, backup di sistema, database di posta, dischi rigidi, unità rimovibili e unità di rete.

Scansione rapida

Scansione anti-virus degli oggetti di avvio del sistema operativo.

AGGIORNAMENTO

Per bloccare eventuali attacchi di rete, eliminare un virus o un altro programma dannoso, è necessario che Kaspersky Anti-Virus venga aggiornato regolarmente. Il componente **Aggiornamenti** è progettato per questo scopo. Consente infatti di gestire l'aggiornamento dei moduli e dei database utilizzati dall'applicazione.

Il servizio di distribuzione degli aggiornamenti consente di salvare gli aggiornamenti dei moduli di programma e dei database scaricati dai server di Kaspersky Lab in una cartella locale in modo da consentire ad altri computer della rete l'accesso agli aggiornamenti e ridurre quindi il traffico di rete.

FUNZIONI DI ASSISTENZA DELL'APPLICAZIONE

Kaspersky Anti-Virus comprende un insieme di funzionalità di assistenza Progettate. Progettate per mantenere aggiornata la protezione del computer, espandere le funzionalità dell'applicazione e fornire un supporto per il relativo utilizzo.

File di dati e rapporti

Durante l'utilizzo dell'applicazione viene creato un rapporto da ogni componente della protezione, attività di scansione e aggiornamento dell'applicazione. Tale rapporto contiene informazioni sulle attività eseguite e i relativi risultati. I dati forniti consentono di conoscere nei dettagli il funzionamento dei singoli componenti di Kaspersky Anti-

Virus. In caso di problemi, è possibile inviare i rapporti a Kaspersky Lab. Gli specialisti potranno approfondire la situazione e trovare una soluzione in tempi più brevi.

Kaspersky Anti-Virus sposta tutti i file sospetti in un'area di archiviazione speciale denominata *Quarantena*. I file vengono memorizzati in forma crittografata per evitare di infettare il computer. È possibile eseguire la scansione anti-virus di questi oggetti, ripristinarli nella posizione precedente, eliminarli oppure aggiungere file all'area della quarantena. Tutti i file che il completamento della scansione anti-virus dimostra essere non infetti vengono automaticamente ripristinati nella posizione precedente.

La cartella *Backup* include le copie dei file disinfettati ed eliminati da Kaspersky Anti-Virus. Tali copie vengono create al fine di ripristinare, se necessario, i file o un'immagine da un'infezione. Le copie di backup dei file vengono inoltre archiviate in forma crittografata per evitare ulteriori infezioni.

È possibile ripristinare un file dalla copia di backup nella posizione originale ed eliminare la copia.

Disco di Ripristino

Disco di Ripristino è stato progettato per eseguire la scansione dei computer compatibili con le piattaforme x86 e per disinfettarli. È consigliabile utilizzare l'applicazione quando il livello di infezione è tale da reputare impossibile la disinfezione tramite applicazioni anti-virus o utilità di rimozione di malware.

Licenza

Quando si acquista Kaspersky Anti-Virus, si stipula un contratto di licenza con Kaspersky Lab che regola l'utilizzo dell'applicazione, l'accesso agli aggiornamenti dei database dell'applicazione e l'assistenza tecnica per un periodo di tempo specificato. I termini di utilizzo e le altre informazioni necessarie per la piena funzionalità dell'applicazione vengono forniti nella licenza.

Utilizzando la funzione **Licenza**, è possibile ottenere informazioni dettagliate sulla propria licenza e acquistare una nuova licenza o rinnovare quella corrente.

Assistenza tecnica

Tutti gli utenti registrati di Kaspersky Anti-Virus possono avvalersi del servizio di assistenza tecnica. Per visualizzare le informazioni sui centri in cui ricevere assistenza tecnica, utilizzare la funzione **Supporto**.

Mediante i seguenti collegamenti, è possibile accedere al forum degli utenti dei prodotti Kaspersky Lab e inviare un rapporto di errore all'assistenza tecnica o un feedback sull'applicazione tramite uno speciale modulo online.

È inoltre possibile accedere ai Servizi di assistenza personalizzata e al servizio di assistenza tecnica online. Il nostro personale sarà sempre lieto di fornire assistenza telefonica per Kaspersky Anti-Virus.

INSTALLAZIONE DI KASPERSKY ANTI-VIRUS 6.0

È possibile installare Kaspersky Anti-Virus 6.0 per Windows Workstations MP4 su un computer in diversi modi:

- installazione locale – installazione dell'applicazione su un unico computer. Per eseguire e completare l'installazione è necessario l'accesso diretto a quel determinato computer. L'installazione locale può essere eseguita in una delle modalità indicate di seguito:
  - modalità interattiva, tramite l'installazione guidata dell'applicazione (vedere la sezione "Installazione mediante procedura guidata" a pag. 20). Tale modalità richiede la partecipazione dell'utente durante l'installazione;
  - modalità non-interattiva in cui l'installazione dell'applicazione viene avviata da riga di comando e non richiede la partecipazione dell'utente durante l'installazione (vedere la sezione "Installazione dell'applicazione da riga di comando" a pag. 24).
- installazione remota – l'installazione dell'applicazione su computer in rete gestiti in remoto dalla workstation dell'amministratore mediante:
  - il set di programmi di Kaspersky Administration Kit (vedere il manuale Kaspersky Administration Kit Deployment Guide);
  - criteri del dominio di gruppo di Microsoft Windows Server 2000/2003 (vedere la sezione "Installazione dall'editor Oggetti criteri di gruppo " a pag. 24).

Prima dell'avvio dell'installazione di Kaspersky Anti-Virus (inclusa quella remota), si raccomanda di chiudere tutte le applicazioni attive.

IN QUESTA SEZIONE

Installazione tramite procedura guidata 20

Installazione dell'applicazione da riga di comando 24

Installazione dall'editor Oggetti criteri di gruppo 24

INSTALLAZIONE TRAMITE PROCEDURA GUIDATA

Per installare Kaspersky Anti-Virus sul computer, eseguire il file di installazione che si trova nel CD del prodotto.

L'installazione dell'applicazione dal file di installazione scaricato da Internet è identica a quella da CD.

Il programma di installazione viene implementato come una procedura guidata standard di Windows. In ogni finestra è disponibile presente un insieme di pulsanti per il controllo del processo di installazione. Di seguito vengono descritte in breve le funzioni di ciascun pulsante:

- **Avanti** – accetta l'azione e passa al punto successivo della procedura di installazione.
- **Indietro** – torna al punto precedente della procedura di installazione.
- **Annulla** – annulla l'installazione.

- **Fine** – completa la procedura di installazione dell'applicazione.

Di seguito è fornita una descrizione dettagliata di ciascun punto dell'installazione del pacchetto.

PASSAGGIO 1. VERIFICA DEI REQUISITI DI INSTALLAZIONE DEL SISTEMA

Prima di installare Kaspersky Anti-Virus, la procedura guidata verificherà che il computer soddisfi i requisiti minimi. Inoltre, verificherà anche le autorizzazioni necessarie per l'installazione del software.

Se uno dei requisiti non viene soddisfatto, sullo schermo verrà visualizzato il messaggio corrispondente. Si raccomanda di installare gli aggiornamenti e i programmi necessari mediante il servizio **Windows Update,** prima di avviare nuovamente l'installazione di Kaspersky Anti-Virus.

PASSAGGIO 2. FINESTRA DI AVVIO DELL'INSTALLAZIONE

Se il sistema soddisfa totalmente i requisiti di base, subito dopo l'esecuzione del file di installazione verrà visualizzata la finestra di avvio contenente le informazioni sull'avvio dell'installazione di Kaspersky Anti-Virus.

Per procedere con l'installazione, fare clic sul pulsante **Avanti.** Per annullare l'installazione, fare clic sul pulsante **Annulla**.

PASSAGGIO 3. VISUALIZZAZIONE DEL CONTRATTO DI LICENZA

La finestra di dialogo successiva dell'applicazione contiene il contratto di licenza tra l'utente e Kaspersky Lab. Si raccomanda di leggerlo con attenzione e, se si accettano tutti i termini e le condizioni del contratto, selezionare l'opzione **Accetto i termini del contratto di licenza**, quindi fare clic sul pulsante **Avanti**. L'installazione continua.

Per annullare l'installazione, fare clic sul pulsante **Annulla**.

PASSAGGIO 4. SELEZIONE DELLA CARTELLA DI INSTALLAZIONE

Nel passaggio successivo dell'installazione di Kaspersky Anti-Virus viene definita la cartella di installazione dell'applicazione. Il percorso predefinito è il seguente:

- **<Unità>** → **Tutti i programmi** → **Kaspersky Lab** → **Kaspersky Anti-Virus 6.0 per Windows Workstations MP4** – per i sistemi a 32 bit.

- **<Unità>** → **Programmi (x86)** → **Kaspersky Lab** → **Kaspersky Anti-Virus 6.0 per Windows Workstations MP4** – per i sistemi a 64 bit.

È possibile specificare una cartella diversa scegliendo il pulsante **Sfoglia** e selezionando una cartella nella finestra di selezione standard oppure immettendo il percorso della cartella nel relativo campo di immissione.

Se si inserisce manualmente il percorso completo della cartella di installazione, la cui lunghezza non deve superare i 200 caratteri e non deve contenere caratteri speciali.

Per procedere con l'installazione, fare clic sul pulsante **Avanti.**

PASSAGGIO 5. UTILIZZO DELLE IMPOSTAZIONI DELL'APPLICAZIONE SALVATE DOPO UN'INSTALLAZIONE PRECEDENTE

In questo passaggio, è possibile specificare se, per il funzionamento dell'applicazione, si desidera utilizzare le impostazioni di protezione, i database dell'applicazione e il database Anti-Spam, se tali oggetti sono stati salvati sul computer dopo la rimozione della versione precedente di Kaspersky Anti-Virus 6.0.

Verrà ora illustrato in dettaglio come abilitare le funzionalità descritte prima.

Se sono stati salvati i database dopo la rimozione di una versione precedente (build) di Kaspersky Anti-Virus, è possibile integrarli nella versione che si sta installando. Per eseguire questa operazione, selezionare la casella ☑ **Database dell'applicazione**. I database dell'applicazione inclusi nel pacchetto di installazione non verranno copiati sul computer.

Per utilizzare le impostazioni di protezione modificate in una versione precedente e salvate sul computer, selezionare la casella ☑ **Impostazioni applicazione**.

È inoltre consigliabile utilizzare il database Anti-Spam se questo è stato salvato dopo la rimozione della versione precedente dell'applicazione. In questo modo sarà possibile ignorare la procedura di addestramento Anti-Spam. Per riutilizzare il database creato in precedenza, selezionare la casella ☑ **Database Anti-Spam**.

PASSAGGIO 6. SELEZIONE DEL TIPO DI INSTALLAZIONE

In questo passaggio, è necessario specificare la completezza dell'installazione dell'applicazione. È possibile scegliere tra due opzioni di installazione:

- **Completa**. In questo caso, tutti i componenti di Kaspersky Anti-Virus verranno installati sul computer. Per conoscere i passaggi seguenti dell'installazione, fare riferimento al Passaggio 8.
- **Personalizzato**. In questo caso, è possibile selezionare i componenti dell'applicazione che si desidera installare. Per ulteriori dettagli, vedere il Passaggio 7.

Per selezionare la modalità di installazione, fare clic sul pulsante corrispondente.

PASSAGGIO 7. SELEZIONE DEI COMPONENTI DELL'APPLICAZIONE PER L'INSTALLAZIONE

Questo passaggio verrà eseguito esclusivamente se è stata selezionata l'opzione di installazione **Personalizzato**.

Prima dell'avvio dell'installazione personalizzata, è necessario selezionare i componenti di Kaspersky Anti-Virus che si desidera installare. Per impostazione predefinita, tutti i componenti di protezione, il componente Scansione virus e il connettore Network Agent per gestire l'applicazione in remoto tramite Kaspersky Administration Kit sono selezionati per l'installazione.

Per selezionare un componente per una installazione successiva, è necessario aprire il menu facendo clic sull'icona che si trova accanto al nome del componente e scegliere la voce **La funzionalità specificata sarà installata sull'unità disco fisso locale**. Nella parte inferiore della finestra del programma di installazione sono contenute le informazioni sul tipo di protezione fornite dal componente selezionato e lo spazio di archiviazione necessario per l'installazione.

Per informazioni dettagliate sullo spazio disco disponibile sul computer, premere il pulsante **Volume**. Le informazioni vengono visualizzate nella finestra aperta.

Per annullare l'installazione dei componenti, selezionare l'opzione **La funzionalità specificata diventerà non disponibile** dal menu di scelta rapida. Se si annulla l'installazione di un componente, il computer non sarà protetto contro diversi programmi pericolosi.

Al termine della selezione dei componenti da installare, premere il pulsante **Avanti.** Per tornare all'elenco predefinito dei componenti da installare, premere il pulsante **Reimposta.**

PASSAGGIO 8. DISABILITAZIONE DEL FIREWALL DI MICROSOFT WINDOWS

Questo passaggio deve essere eseguito solo se l'installazione di Kaspersky Anti-Virus avviene su un computer in cui è stato abilitato il firewall e in cui si prevede di installare il componente Anti-Hacker.

A questo punto dell'installazione di Kaspersky Anti-Virus, verrà data la possibilità di disabilitare il firewall di Microsoft Windows, poiché il componente Anti-Hacker garantisce protezione completa all'attività di rete e non c'è nessuna esigenza di creare una protezione aggiuntiva all'interno dello stesso sistema operativo.

Se si desidera utilizzare Anti-Hacker come strumento di protezione principale per l'attività di rete, premere il pulsante **Avanti**. Il firewall di Microsoft Windows verrà disabilitato automaticamente.

Se si desidera proteggere il computer con il firewall di Microsoft Windows, selezionare l'opzione **Non disabilitare Windows Firewall**. In tal caso, il componente Anti-Hacker verrà installato, ma disabilitato per evitare conflitti nel funzionamento delle applicazioni.

PASSAGGIO 9. RICERCA DI ALTRE APPLICAZIONI ANTI-VIRUS

A questo punto, la procedura guidata cercherà altri programmi anti-virus, inclusi altri programmi di Kaspersky Lab, che potrebbero entrare in conflitto con Kaspersky Anti-Virus.

Se sul computer vengono rilevate applicazioni anti-virus, queste ultime verranno elencate sullo schermo. Prima di proseguire con l'installazione, l'utente avrà la possibilità di disinstallarle.

È possibile scegliere di rimuoverle automaticamente o manualmente, mediante i controlli che si trovano sotto l'elenco dei programmi anti-virus rilevati.

Per procedere con l'installazione, fare clic sul pulsante **Avanti.**

PASSAGGIO 10. PREPARAZIONE FINALE PER L'INSTALLAZIONE

Questo passaggio completa la preparazione per l'installazione dell'applicazione sul computer.

Per l'installazione iniziale di Kaspersky Anti-Virus 6.0, si consiglia di non deselezionare la casella **Proteggi il processo di installazione**. Tale protezione, infatti, consente l'esecuzione della procedura corretta del rollback dell'installazione selezionare nel caso in cui si verifichino errori durante l'operazione. Durante un nuovo tentativo di installazione di un'applicazione, si consiglia di non deselezionare questa casella.

Se l'applicazione viene installata in remoto mediante il **Desktop remoto di Windows**, è consigliabile deselezionare la casella
Proteggere il processo di installazione. In caso contrario, la procedura di installazione potrebbe essere eseguita in maniera non corretta o non completata affatto.

Per procedere con l'installazione, fare clic sul pulsante **Installa**.

Durante l'installazione dei componenti di Kaspersky Anti-Virus che intercettano traffico di rete, vengono terminate le connessioni di rete correnti. La maggior parte delle connessioni terminate verrà ripristinata regolarmente.

PASSAGGIO 11. COMPLETAMENTO DELL'INSTALLAZIONE

La finestra **Installazione completa** contiene informazioni sul completamento dell'installazione di Kaspersky Anti-Virus sul computer.

Per eseguire la Configurazione guidata iniziale, premere il pulsante **Avanti**.

Se per completare con successo l'installazione viene richiesto di riavviare il computer, viene visualizzata una notifica speciale.

INSTALLAZIONE DELL'APPLICAZIONE DA RIGA DI COMANDO

- *Per installare Kaspersky Anti-Virus 6.0 per Windows Workstation MP4, digitare la seguente riga di comando:*

```
msiexec /i <nome_pacchetto>
```

Verrà eseguita l'installazione guidata (vedere la sezione "Installazione mediante procedura guidata" a pag. 20). Al termine dell'installazione dell'applicazione, viene richiesto il riavvio del computer.

- *Per eseguire l'installazione in modalità non interattiva (senza avviare la procedura guidata), digitare quanto segue:*

```
msiexec /i <nome_pacchetto> /qn
```

In tal caso, il computer deve essere riavviato manualmente al termine dell'installazione dell'applicazione. Per riavviare automaticamente il computer, digitare la seguente riga di comando:

```
msiexec /i <nome_pacchetto> ALLOWREBOOT=1 /qn
```

È possibile eseguire il riavvio automatico solo nella modalità di installare non interattiva (con il comando /qn).

- *Per installare l'applicazione con una password, che conferma l'autorizzazione a rimuovere l'applicazione, digitare quanto segue:*

  `msiexec /i <nome_pacchetto> KLUNINSTPASSWD=******` – per l'installazione dell'applicazione in modalità interattiva;

  `msiexec /i <nome_pacchetto> KLUNINSTPASSWD=****** /qn` – per l'installazione dell'applicazione in modalità non interattiva senza riavviare il computer;

  `msiexec /i <nome_pacchetto> KLUNINSTPASSWD=****** ALLOWREBOOT=1 /qn` – per l'installazione dell'applicazione in modalità non interattiva con riavvio del computer.

Per l'installazione di Kaspersky Anti-Virus in modalità non interattiva, è supportata la lettura del file setup.ini (vedere pagina 25). Tale file contiene impostazioni generali per l'installazione dell'applicazione, il file di configurazione *instal.cfg* (vedere la sezione "Importazione delle impostazioni di protezione" a pag. 204) e il file della chiave di licenza. Tali file devono trovarsi nella stessa cartella del pacchetto di installazione di Kaspersky Anti-Virus.

INSTALLAZIONE DALL'EDITOR OGGETTI CRITERI DI GRUPPO

Mediante l'**editor Oggetti criteri di gruppo** è possibile installare, aggiornare e rimuovere Kaspersky Anti-Virus su workstation aziendali appartenenti al dominio, senza l'impiego di Kaspersky Administration Kit.

INSTALLAZIONE DELL'APPLICAZIONE

Per installare Kaspersky Anti-Virus, eseguire le seguenti operazioni:

1. Creare una cartella di rete condivisa sul computer, che agirà da controller di dominio, e inserirvi il pacchetto di installazione di Kaspersky Anti-Virus in formato.*msi*.

   Inoltre, in tale directory è possibile inserire il file *setup.ini* (vedere pagina 25), contenente l'elenco delle impostazioni dell'installazione di Kaspersky Anti-Virus, il file di configurazione *install.cfg* (vedere la sezione "Importazione delle impostazioni di protezione" a pag. 204) e il file della chiave di licenza.

2. Dalla console standard MMC, aprire l'**editor Oggetti criteri di gruppo** (per informazioni dettagliate sul funzionamento di questo editor fare riferimento al sistema di Guida di Microsoft Windows).

3. Creare un nuovo pacchetto. Per eseguire questa operazione, selezionare **Oggetti criteri di gruppo / Configurazione del computer/ Configurazione dell'applicazione / Installazione del software** dalla struttura ad albero della console e utilizzare il comando **Crea / Pacchetto** dal menu di scelta rapida.

   Nella finestra visualizzata, specificare il percorso della cartella di rete condivisa in cui si trova il pacchetto di installazione di Kaspersky Anti-Virus. Nella finestra di dialogo **Distribuzione dell`applicazione**, selezionare l'impostazione **Assegnata**, quindi premere il pulsante **OK**.

I criteri di gruppo verranno applicati a ciascuna workstation alla successiva registrazione di computer nel dominio. Di conseguenza, Kaspersky Anti-Virus verrà installato su tutti i computer.

DESCRIZIONE DELLE IMPOSTAZIONI DEL FILE SETUP.INI

Il file *setup.ini*, che si trova nella directory del pacchetto di installazione di Kaspersky Anti-Virus, viene utilizzato per l'installazione dell'applicazione in modalità non interattiva da riga di comando o dall'editor Oggetti criteri di gruppo. Tale file contiene le impostazioni indicate di seguito:

[Setup] – impostazioni generali per l'installazione dell'applicazione.

- **InstallDir=**<percorso della cartella di installazione dell'applicazione>.
- **Reboot=yes|no** – definisce se il computer deve riavviarsi al termine dell'installazione dell'applicazione (il riavvio non viene eseguito per impostazione predefinita).
- **SelfProtection=yes|no** – definisce se la funzione di Auto-difesa di Kaspersky Anti-Virus deve essere abilitata durante l'installazione (la funzione è abilitata per impostazione predefinita).
- **NoKLIM5=yes|no** – definisce se l'installazione dei driver di rete di Kaspersky Anti-Virus deve essere annullata durante l'installazione dell'applicazione (i driver vengono installati per impostazione predefinita). I driver di rete di Kaspersky Anti-Virus di tipo NDIS, che intercettano il traffico di rete per componenti dell'applicazione, quali Anti-Hacker, Anti-Virus Posta, Web Anti-Virus e Anti-Spam, possono causare conflitti con altre applicazione o dispositivi installati sul computer dell'utente. È possibile non procedere all'installazione dei driver di rete su computer che eseguono Microsoft Windows XP o Microsoft Windows 2000 per evitare probabili conflitti.

  Tale opzione non è disponibile su computer che eseguono Microsoft in XP x64 Edition o Microsoft Windows Vista.

[Components] – selezione di componenti dell'applicazione da installare. Se non è specificato alcun componente, l'applicazione verrà installata integralmente. Se è specificato almeno un componente, i componenti non presenti in elenco non verranno installati.

- **FileMonitor=yes|no** – installazione del componente Anti-Virus File.
- **MailMonitor=yes|no** – installazione del componente Anti-Virus Posta.
- **WebMonitor=yes|no** – installazione del componente Web Anti-Virus.

- **ProactiveDefence=yes|no** – installazione del componente Difesa Proattiva.
- **AntiSpy=yes|no** – installazione del componente Anti-Spy.
- **AntiHacker=yes|no** – installazione del componente Anti-Hacker.
- **AntiSpam=yes|no** – installazione del componente Anti-Spam.
- **LockControl=yes|no** – installazione del componente Controllo dispositivo.

[Tasks] – abilitazione attività di Kaspersky Anti-Virus. Se non è specificata alcuna attività, al termine dell'installazione verranno abilitate tutte le attività. Se è specificata almeno un'attività, quelle non presenti in elenco non verranno installate.

- **ScanMyComputer=yes|no** – attività di scansione completa.
- **ScanStartup=yes|no** – attività di scansione rapida.
- **Scan=yes|no** – attività di scansione.
- **Updater=yes|no** – attività di aggiornamento per i database e i moduli del programma.

È possibile utilizzare i valori 1, on, enable, enabled anziché il valore **yes** e il valore 0, off, disable, disabled anziché il valore **no**.

AGGIORNAMENTO DELLA VERSIONE DELL'APPLICAZIONE

Per aggiornare la versione di Kaspersky Anti-Virus, eseguire le seguenti operazioni:

1. Inserire in una cartella di rete condivisa il pacchetto di installazione contenente gli aggiornamenti di Kaspersky Anti-Virus in formato MSI.
2. Aprire l'**editor Oggetti criteri di gruppo** e creare un nuovo pacchetto mediante la procedura descritta in precedenza.
3. Selezionare il nuovo pacchetto dall'elenco e utilizzare il comando **Proprietà** dal menu di scelta rapida. Selezionare la scheda **Aggiornamenti** nella finestra delle proprietà del pacchetto e specificare il pacchetto contenente il pacchetto di installazione della versione precedente di Kaspersky Anti-Virus. Per installare una versione aggiornata di Kaspersky Anti-Virus salvando le impostazioni di protezione, selezionare l'opzione di installazione con sovrascrittura del pacchetto esistente.

I criteri di gruppo verranno applicati a ciascuna workstation alla successiva registrazione di computer nel dominio.

RIMOZIONE DELL'APPLICAZIONE

Per rimuovere Kaspersky Anti-Virus, eseguire le seguenti operazioni:

1. Aprire **editor Oggetti criteri di gruppo**.
2. Selezionare **Oggetti criteri di gruppo / Configurazione del computer/ Configurazione dell'applicazione / Installazione del software** nella struttura ad albero della console.

   Selezionare il pacchetto di Kaspersky Anti-Virus dall'elenco, aprire il menu di scelta rapida ed eseguire **Tutte le attività/ Rimuovi** command.

Nella finestra di dialogo **Rimozione applicazioni in corso**, selezionare **Rimuovere immediatamente l'applicazione dai computer di tutti gli utenti**, di modo che Kaspersky Anti-Virus verrà rimosso al riavvio successivo.

OPERAZIONI PRELIMINARI

Durante la creazione di Kaspersky Anti-Virus, gli specialisti di Lab si sono posti l'obiettivo, tra gli altri, di fornire la configurazione ottimale dell'applicazione. Ciò consente agli utenti, indipendentemente dalle loro conoscenze in ambito informatico, di garantire in tempi rapidi e in poche mosse la protezione del computer subito dopo l'installazione.

Tuttavia, i dettagli di configurazione del computer o delle attività da eseguire con l'applicazione possono presentare aspetti specifici. Per questo motivo, si consiglia di eseguire una configurazione preliminare al fine di ottenere l'approccio più flessibile e personalizzato per la protezione del computer.

Per agevolare l'utente, le fasi di configurazione preliminari sono state combinate nell'interfaccia unificata della Configurazione guidata iniziale che si avvia subito dopo il completamento della procedura di installazione dell'applicazione. Seguendo le istruzioni della procedura guidata, è possibile attivare l'applicazione, modificare le impostazioni di aggiornamento, limitare l'accesso all'applicazione tramite una password e modificare altre impostazioni.

Il computer può essere infettato da malware prima che venga installato Kaspersky Anti-Virus. Per rilevare malware, eseguire la scansione del computer (vedere la sezione "Scansione anti-virus del computer" a pag. 124).

Al momento dell'installazione dell'applicazione i database inclusi nel pacchetto di installazione potrebbero inoltre diventare obsoleti. Avviare l'aggiornamento dell'applicazione (a pag. 135), a meno che tale operazione non sia stata già eseguita mediante la configurazione guidata o automaticamente subito dopo l'installazione dell'applicazione.

Il componente Anti-Spam incluso nel pacchetto di Kaspersky Anti-Virus utilizza un algoritmo di autoaddestramento per rilevare i messaggi indesiderati. Eseguire l'Addestramento guidato Anti-Spam (vedere la sezione "Addestramento di Anti-Spam mediante l'addestramento guidato" a pag. 106) per configurare il componente per l'utilizzo della posta.

Al termine delle azioni previste in questa sezione, l'applicazione sarà pronta a proteggere il computer. Per valutare il livello di protezione del computer, utilizzare la Gestione guidata della protezione (vedere la sezione "Gestione della protezione a pag. 35).

IN QUESTA SEZIONE

Configurazione guidata iniziale 28

Scansione anti-virus del computer 34

Aggiornamento dell'applicazione 34

Gestione delle licenze 35

Gestione della protezione 35

Sospendi protezione 36

Eliminazione dei problemi. Assistenza tecnica utente 37

Creazione di un file di traccia 37

Configurazione delle impostazioni dell'applicazione 38

Rapporti sul funzionamento dell'applicazione. File di dati 38

CONFIGURAZIONE GUIDATA INIZIALE

La configurazione guidata di Kaspersky Anti-Virus viene avviata al termine dell'installazione dell'applicazione. È progettata per consentire la configurazione delle impostazioni iniziali dell'applicazione, in base alle funzioni e alle attività del computer.

L'interfaccia della configurazione guidata riprende quella standard della procedura guidata di Microsoft Windows e consiste in una serie di passaggi che è possibile visualizzare mediante i pulsanti **Indietro** e **Avanti** o terminare mediante il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

Per terminare l'installazione dell'applicazione nel computer, è necessario eseguire tutti i passaggi della procedura guidata. Se le operazioni della procedura guidata vengono interrotte per qualche motivo, i valori delle impostazioni già specificati non verranno salvati. Al successivo tentativo di esecuzione dell'applicazione, viene riavviata la configurazione guidata iniziale per modificare nuovamente le impostazioni.

UTILIZZO DEGLI OGGETTI SALVATI DALLA VERSIONE PRECEDENTE

Questa finestra della procedura guidata viene visualizzata quando si installa l'applicazione su una versione precedente di Kaspersky Anti-Virus. È possibile scegliere quali dati utilizzati nella versione precedente devono essere importati nella nuova versione. Tali dati possono essere oggetti in quarantena o del backup oppure impostazioni di protezione.

Per utilizzare quei dati nella nuova versione dell'applicazione, selezionare tutte le caselle necessarie.

ATTIVAZIONE DELL'APPLICAZIONE

La procedura di attivazione dell'applicazione consiste nella registrazione di una licenza mediante l'installazione di un file chiave. A seconda della licenza in uso, l'applicazione determinerà i privilegi esistenti e ne calcolerà le condizioni di utilizzo.

Il file chiave contiene informazioni di servizio necessarie per fare in modo che Kaspersky Anti-Virus sia completamente funzionale, nonché dati aggiuntivi:

- informazioni di assistenza, ovvero chi fornisce assistenza e dove può essere ottenuta;
- nome e numero della chiave e data di scadenza della licenza.

In base alla presenza di un file chiave o meno (nel caso in cui il file debba essere ricevuto dal server di Kaspersky Lab), saranno disponibili le seguenti opzioni per l'attivazione di Kaspersky Anti-Virus:

- Attivazione online (vedere a pag. 29). Selezionare questa opzione se è stata acquistata una versione in commercio dell'applicazione ed è stato ottenuto un codice di attivazione. È possibile utilizzare tale codice per ottenere un file chiave per l'accesso alle funzionalità complete dell'applicazione per tutto il periodo di validità della licenza.
- Attivazione della versione di prova (vedere a pag. 30). Utilizzare questa opzione di attivazione se si desidera installare la versione di prova dell'applicazione prima di procedere all'acquisto di una versione in commercio. Verrà fornito un file chiave gratuito valido per un periodo specificato nel contratto di licenza della versione di prova.
- Attivazione mediante un file chiave di licenza ottenuto in precedenza (vedere la sezione "Attivazione tramite un file chiave" a pag. 30). Attivare l'applicazione mediante il file chiave di Kaspersky Anti-Virus 6.0 ottenuto in precedenza.
- Attivare successivamente. Se si sceglie questa opzione, la fase di attivazione verrà ignorata. L'applicazione sarà installata sul computer e sarà possibile accedere a tutte le funzioni del programma ad eccezione degli aggiornamenti (sarà disponibile un solo aggiornamento dell'applicazione subito dopo l'installazione). L'opzione **Attivare successivamente** è disponibile solo al primo avvio dell'Attivazione guidata. Agli avvii successivi della procedura guidata, se l'applicazione risulta già attivata, sarà disponibile l'opzione **Elimina file di chiave** per eseguire la rimozione.

Se le prime due opzioni di attivazione dell'applicazione sono entrambe selezionate, l'applicazione verrà attivata tramite il server Web di Kaspersky Lab. Tale operazione richiede la connessione a Internet. Prima di avviare l'attivazione, verificare e modificare, se necessario, le impostazioni di connessione alla rete nella finestra che verrà visualizzata premendo il pulsante **Impostazioni LAN**. Per ulteriori dettagli sulle impostazioni di rete, contattare l'amministratore di rete o il provider Internet.

Se, al momento dell'installazione non è disponibile una connessione Internet, è possibile eseguire l'attivazione successivamente, tramite l'interfaccia dell'applicazione oppure mediante connessione a Internet da un computer diverso per ottenere una chiave, utilizzando un codice di attivazione ricevuto mediante registrazione al sito Web del servizio di assistenza tecnica di Kaspersky Lab.

È inoltre possibile attivare l'applicazione tramite il Kaspersky Administration Kit. Per effettuare questa operazione, è necessario creare un'attività di installazione del file chiave (vedere pagina 220). Per ulteriori dettagli fare riferimento alla guida di Kaspersky Administration Kit.

VEDERE ANCHE

Attivazione online 29

Come ottenere un file chiave 29

Attivazione tramite un file chiave 30

Completamento dell'attivazione 30

ATTIVAZIONE ONLINE

L'attivazione online viene eseguita immettendo un codice di attivazione inviato tramite e-mail per l'acquisto di Kaspersky Anti-Virus tramite Internet. Se si acquista l'applicazione in confezione presso un rivenditore, il codice di attivazione è stampato sulla custodia cartacea del disco di installazione.

IMMISSIONE DEL CODICE DI ATTIVAZIONE

A questo punto, è necessario immettere il codice di attivazione. Tale codice è una sequenza di numeri e lettere divisi da trattini in quattro gruppi di cinque simboli senza spazi. Ad esempio, 11111-11111-11111-11111. Il codice deve essere immesso in caratteri dell'alfabeto latino.

Immettere le informazioni personali nella parte inferiore della finestra: nome completo, indirizzo e-mail, stato e città di residenza. Queste informazioni potrebbero essere necessarie per identificare un utente registrato se, ad esempio, la licenza è stata smarrita o rubata. In tal caso, è possibile ottenere un altro codice di attivazione tramite le informazioni personali.

COME OTTENERE UN FILE CHIAVE

La configurazione guidata esegue la connessione ai server Internet di Kaspersky Lab e invia i dati di registrazione, tra cui il codice di attivazione e le informazioni di contatto. Una volta stabilita la connessione, il codice di attivazione e le informazioni di contatto vengono verificate. Se il codice di attivazione viene accettato, si riceve un file chiave della licenza che verrà quindi installato automaticamente. Al termine dell'attivazione, viene visualizzata la finestra contenente le informazioni dettagliate sulla licenza ottenuta.

Se il codice di attivazione non viene accettato, viene visualizzato il relativo avviso. in questo caso, contattare il rivenditore del software presso il quale è stato effettuato l'acquisto per le informazioni del caso.

Se viene superato il numero consentito di attivazioni con il codice di attivazione specifico, viene visualizzato il relativo avviso. Il processo di attivazione viene interrotto e l'applicazione consente di contattare il servizio Assistenza tecnica di Kaspersky Lab.

ATTIVAZIONE DELLA VERSIONE DI PROVA

Utilizzare questa opzione di attivazione se si desidera installare una versione di prova di Kaspersky Anti-Virus prima di procedere all'acquisto di una versione commerciale. Verrà fornita una licenza gratuita che sarà valida per il periodo specificato nel contratto di licenza della versione di prova. Alla scadenza della licenza, non sarà possibile attivare nuovamente la versione di prova.

ATTIVAZIONE TRAMITE UN FILE CHIAVE

Se si dispone di file chiave, è possibile utilizzarlo per attivare Kaspersky Anti-Virus. Per effettuare questa operazione, premere il pulsante **Sfoglia** e selezionare il percorso del file con estensione *.key*.

Dopo aver installato la chiave, nella parte inferiore della finestra verranno visualizzate le informazioni sulla licenza: numero della licenza, tipo di licenza (commerciale, beta, di prova e così via), data di scadenza della licenza e numero di host.

COMPLETAMENTO DELL'ATTIVAZIONE

La configurazione guidata informa l'utente che Kaspersky Anti-Virus è stato attivato correttamente. Vengono inoltre fornite informazioni sulla licenza: numero della licenza, tipo di licenza (commerciale, beta, di prova e così via), data di scadenza e numero di host.

MODALITÀ DI PROTEZIONE

In questa finestra della configurazione guidata viene chiesto di selezionare la modalità di protezione in cui dovrà operare l'applicazione:

- **Protezione di base**. Questa è la modalità predefinita progettata per gli utenti che non hanno grande esperienza di computer e software anti-virus. Tutti i componenti dell'applicazione vengono impostati sui livelli di protezione consigliati e informano l'utente solo in caso di eventi pericolosi, quali il rilevamento di codice dannoso o l'esecuzione di azioni pericolose.

- **Protezione interattiva**. Questa modalità consente di impostare una difesa più personalizzata dei dati del computer rispetto alla modalità di base. Consente il monitoraggio dei tentativi di modifica delle impostazioni di sistema, dell'attività di sistema sospetta e delle operazioni non autorizzate sulla rete.

  Ciascuna di queste azioni può essere provocata dall'attività di un programma dannoso o essere una caratteristica standard per il funzionamento delle applicazioni installate sul computer. L'utente dovrà decidere per ogni singolo caso se tali attività devono essere autorizzate o bloccate.

  Se si seleziona questa modalità, è necessario specificare in quali casi deve essere utilizzata:

  - **Abilita modalità Apprendimento Anti-Hacker** chiede di accettare le azioni nelle situazioni in cui i programmi installati sul computer tentano di connettersi a una risorsa di rete. È possibile consentire o bloccare la connessione e configurare regole Anti-Hacker per quell'applicazione. Se si disabilita la modalità di addestramento, Kaspersky Anti-Virus viene eseguito con le impostazioni minime di protezione. Ciò significa che consente a tutte le applicazioni di accedere alle risorse di rete.

  - **Abilita Controllo del Registro** chiede una reazione a ogni rilevamento di tentativi di modifica degli oggetti del registro di sistema.

CONFIGURAZIONE DELLE IMPOSTAZIONI DI AGGIORNAMENTO

L'efficacia della protezione del computer è strettamente collegata all'esecuzione di aggiornamenti periodici dei database e dei moduli del programma. In questa finestra della procedura guidata viene chiesto di selezionare la modalità di aggiornamento dell'applicazione e di modificare le impostazioni di pianificazione:

- **Automaticamente**. Kaspersky Anti-Virus verifica a intervalli specificati la disponibilità di pacchetti di aggiornamento nell'origine degli aggiornamenti. La frequenza della scansione può essere aumentata quando si verificano periodi di attacchi frequenti e ridotta nei periodi più tranquilli. Se vengono rilevati nuovi aggiornamenti, questi vengono scaricati e installati nel computer. Questa è la modalità predefinita.

- **Ogni 2 ore** (la frequenza può variare in base alle impostazioni di pianificazione). Gli aggiornamenti vengono eseguiti automaticamente in base alla pianificazione. È possibile modificare le impostazioni di pianificazione in un'altra finestra mediante il pulsante **Cambia**.

- **Manualmente**. Se si seleziona questa opzione, gli aggiornamenti verranno eseguiti manualmente.

I database e i moduli dell'applicazione in dotazione con il pacchetto di installazione potrebbero essere obsoleti al momento dell'installazione dell'applicazione. Per questo motivo, si consiglia di procurarsi gli aggiornamenti più recenti dell'applicazione. A tal fine, cliccare su **Aggiorna ora**. A questo punto, dai siti di aggiornamento verranno scaricati gli aggiornamenti necessari e installati sul computer.

Se si desidera passare alla configurazione degli aggiornamenti (specificare le impostazioni di rete, selezionare un'origine di aggiornamento, eseguire un aggiornamento da un account utente specifico o abilitare il download degli aggiornamenti in un'origine locale), premere il pulsante **Impostazioni**.

CONFIGURAZIONE DELLA PIANIFICAZIONE DELLA SCANSIONE ANTI-VIRUS

La scansione delle aree selezionate alla ricerca di oggetti dannosi è una delle attività chiave nella protezione del computer.

Nell'installazione di Kaspersky Anti-Virus, vengono create tre attività di scansione anti-virus predefinite. In questa finestra della configurazione guidata viene chiesto di selezionare una modalità di esecuzione dell'attività di scansione:

Scansione completa

Scansione approfondita dell'intero sistema. Gli oggetti seguenti vengono esaminati per impostazione predefinita: memoria di sistema, programmi caricati all'avvio, backup di sistema, database di posta, dischi rigidi, unità rimovibili e unità di rete. È possibile modificare le impostazioni di pianificazione nella finestra visualizzata premendo il pulsante **Cambia**.

Scansione rapida

Scansione anti-virus degli oggetti di avvio del sistema operativo. È possibile modificare le impostazioni di pianificazione nella finestra visualizzata premendo il pulsante **Cambia**.

LIMITAZIONE DELL'ACCESSO ALL'APPLICAZIONE

Poiché un personal computer può essere usato da più persone, non tutte necessariamente esperte, e poiché i programmi dannosi possono disabilitare la protezione, è possibile proteggere con password l'accesso a Kaspersky Anti-Virus. L'utilizzo di una password consente di proteggere l'applicazione da tentativi non autorizzati di disabilitare la protezione, modificare le impostazioni o disinstallare l'applicazione.

Per abilitare la protezione tramite password, selezionare la casella **Abilita la protezione tramite password** e compilare i campi **Password** e **Conferma password**.

Specificare l'area alla quale si intende applicare la protezione tramite password selezionando una delle opzioni seguenti:

- **Tutte le operazioni (ad eccezione delle notifiche di eventi pericolosi)**. La password verrà richiesta per qualsiasi azione relativa all'applicazione, eccetto che per le risposte alle notifiche di rilevamento di oggetti pericolosi.

- **Operazioni selezionate**:

- ☑ **Configurazione delle impostazioni dell'applicazione** – la password viene richiesta per modificare le impostazioni di Kaspersky Anti-Virus.

- ☑ **Chiusura applicazione in corso** – la password viene richiesta per chiudere l'applicazione.

- ☑ **Disabilitazione dei componenti della protezione e arresto delle attività di scansione** – la password viene richiesta per disabilitare un componente di protezione o interrompere un'attività di scansione.

- ☑ **Disabilitazione dei criteri Kaspersky Administration Kit** – la password viene richiesta per rimuovere il computer dall'ambito dei criteri e delle attività di gruppo (quando si utilizza Kaspersky Administration Kit).

- ☑ **Durante la disinstallazione dell'applicazione** – la password viene richiesta per rimuovere l'applicazione dal computer.

CONFIGURAZIONE DI ANTI-HACKER

Anti-Hacker è il componente di Kaspersky Anti-Virus che protegge il computer sulle reti locali e su Internet. In questa fase, la configurazione guidata offre la possibilità di creare un elenco di regole in grado di guidare Anti-Hacker nell'analisi dell'attività di rete del computer.

VEDERE ANCHE

Determinazione dello stato di una zona di protezione 32

Creazione dell'elenco di applicazioni di rete 33

DETERMINAZIONE DELLO STATO DI UNA ZONA DI PROTEZIONE

In questa fase, la configurazione guidata analizza l'ambiente di rete del computer. In base ai risultati dell'analisi, l'intero spazio di rete viene suddiviso in zone standard:

- *Internet* – il World Wide Web. In questa zona, Kaspersky Anti-Virus opera come firewall personale. Regole predefinite per i pacchetti e le applicazioni disciplinano tutta l'attività di rete per garantire una protezione massima. Quando si lavora in quest'area, le impostazioni di protezione non possono essere modificate, se non per attivare la modalità Mascheramento per una protezione maggiore.

- *Zone di sicurezza* – si tratta di determinate zone standard corrispondenti per lo più alle sottoreti in cui è incluso il computer (sottoreti locali domestiche o al lavoro). Per impostazione predefinita, le attività svolte in queste zone sono definite a medio rischio. È possibile modificare lo stato di queste zone in base a quanto si ritiene affidabile una determinata sottorete, e configurare regole per il filtraggio pacchetti e le applicazioni.

Tutte le zone rilevate vengono visualizzate in un elenco. Ogni zona è accompagnata da una descrizione, l'indirizzo e la maschera di subnet. L'elenco riporta anche lo stato in base al quale ogni attività di rete viene autorizzata o bloccata nell'ambito delle operazioni del componente Anti-Hacker:

- **Internet**. Questo è lo stato predefinito assegnato a Internet, poiché in questa zona il computer è potenzialmente esposto a tutti i tipi di minacce. Si consiglia di selezionare questo stato per le reti non protette da applicazioni anti-virus, firewall, filtri e così via. Quando si seleziona tale stato, l'applicazione garantisce la protezione massima per la zona in questione:

  - blocco di qualsiasi attività di rete NetBIOS all'interno della sottorete;

  - regole Blocca per applicazioni e filtraggio pacchetti che consentono un'attività NetBIOS all'interno della sottorete.

  Anche se è stata creata una cartella condivisa, le informazioni nella stessa non saranno disponibili per utenti appartenenti a sottoreti con questo stato. Inoltre, se questo stato è selezionato per una certa sottorete, non sarà possibile accedere ai file e alle stampanti di altri computer di tale sottorete.

- **Rete locale**. L'applicazione assegna questo stato alla maggior parte delle zone di sicurezza rilevate durante l'analisi dell'ambiente di rete del computer, fatta eccezione per le zone Internet. Questo stato è consigliabile per le aree con un fattore di rischio medio, ad esempio le reti LAN aziendali. Se si seleziona questo stato, l'applicazione consente:

  - qualsiasi attività di rete NetBIOS all'interno della sottorete;

  - l'uso di regole per applicazioni e filtraggio pacchetti che consentono un'attività NetBIOS all'interno della sottorete.

  Selezionare questo stato per consentire l'accesso a certe cartelle o stampanti sul computer ma bloccare qualsiasi altra attività esterna.

- **Attendibili**. Si consiglia di applicare questo stato alle aree che si ritiene siano assolutamente sicure e in cui il computer non è soggetto ad attacchi e tentativi di accesso ai dati. Se si seleziona questo stato, tutte le attività di rete saranno consentite. Anche selezionando la protezione massima e creando regole di blocco, queste non funzioneranno per i computer remoti di un'area attendibile.

È possibile utilizzare la *modalità Mascheramento* per godere di una protezione maggiore quando si usano reti contrassegnate come **Internet**. In questa modalità sono infatti consentite soltanto le attività di rete avviate dal computer in uso, cosicché il computer risulta invisibile per l'ambiente circostante. Questa modalità non pregiudica le prestazioni del computer su Internet.

Si sconsiglia l'uso della modalità Mascheramento se il computer viene utilizzato come server (ad esempio come server di posta o HTTP). Altrimenti i computer che si connettono al server non lo potranno visualizzare all'interno della rete.

Per modificare lo stato di una rete o abilitare / disabilitare la modalità Mascheramento, selezionarla nell'elenco e utilizzare i collegamenti appropriati nella sezione **Descrizione regola** al di sotto dell'elenco. È possibile eseguire operazioni simili e modificare indirizzi e subnet mask nella finestra **Impostazioni zona**, accessibile facendo clic sul pulsante **Modifica**.

È possibile aggiungere una nuova rete all'elenco mentre è visualizzato. Per effettuare questa operazione, premere il pulsante **Aggiorna**. Anti-Hacker cercherà zone disponibili per la registrazione, chiedendo di selezionare uno stato da assegnare a quelle rilevate. È possibile inoltre aggiungere nuove zone all'elenco manualmente (ad esempio se si connette il laptop a una nuova rete). A tale scopo, utilizzare il pulsante **Aggiungi** e immettere le informazioni richieste nella finestra **Impostazioni rete**.

Per eliminare la rete dall'elenco, fare clic sul pulsante **Elimina**.

CREAZIONE DELL'ELENCO DI APPLICAZIONI DI RETE

La configurazione guidata analizza il software installato sul computer e crea un elenco di applicazioni che utilizzano una connessione di rete.

Anti-Hacker crea una regola per controllare l'attività di rete di ogni applicazione di questo tipo. Le regole vengono applicate mediante modelli per le applicazioni più comuni che utilizzano connessioni di rete, creare presso il Kaspersky Lab e in dotazione con il prodotto.

È possibile visualizzare l'elenco delle applicazioni di rete e le regole corrispondenti nella finestra delle impostazioni di Anti-Hacker visualizzabile facendo clic sul pulsante **Applicazioni**.

Per una protezione aggiuntiva, si consiglia di disabilitare la cache DNS durante la navigazione delle risorse di rete. Tale funzione diminuisce drasticamente il tempo necessario al computer per la connessione a una determinata risorsa Internet. Tuttavia, costituisce, allo stesso tempo, una vulnerabilità pericolosa e il suo utilizzo potrebbe consentire a intrusi di provocare perdite di dati non rintracciabili mediante il firewall. Per questo motivo, per aumentare il grado di protezione del computer, si consiglia di disabilitare l'opzione di salvataggio delle informazioni sui nomi di dominio contenute nella cache.

COMPLETAMENTO DELLA CONFIGURAZIONE GUIDATA

L'ultima finestra della procedura guidata chiede all'utente se desidera riavviare il computer per completare l'installazione dell'applicazione. Per registrare i driver di Kaspersky Anti-Virus è necessario riavviare il sistema.

È possibile posticipare il riavvio, ma l'applicazione non sarà completamente funzionale fino al riavvio.

SCANSIONE ANTI-VIRUS DEL COMPUTER

Poiché gli sviluppatori di malware fanno tutto il possibile per nascondere le azioni dei loro programmi, è facile non accorgersi della presenza di tali applicazioni nocive nel computer.

Una volta installato nel computer, Kaspersky Anti-Virus esegue automaticamente l'attività **Scansione rapida**. Questa attività consiste nel cercare e neutralizzare i programmi nocivi negli oggetti caricati all'avvio del sistema.

Gli specialisti di Kaspersky Lab consigliano inoltre di eseguire l'attività di **Scansione completa**.

➡ *Per avviare / interrompere un'attività di scansione anti-virus, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Premere il pulsante **Avvia scansione** per avviare la scansione. Se, durante l'avanzamento dell'attività, è necessario interromperne l'esecuzione, premere il pulsante **Interrompi scansione**.

AGGIORNAMENTO DELL'APPLICAZIONE

Per aggiornare Kaspersky Anti-Virus, è necessario disporre di una connessione a Internet.

L'attività di protezione di Kaspersky Anti-Virus si basa sui database dell'applicazione che contengono firme delle minacce, frasi tipiche dello spam e descrizioni di attacchi di rete. Tali database potrebbero risultare già obsoleti al momento dell'installazione dell'applicazione, poiché Kaspersky Lab aggiorna regolarmente sia i database, che i moduli dell'applicazione.

Quando la configurazione guidata è attiva, è possibile selezionare la modalità di avvio dell'aggiornamento. Per impostazione predefinita, Kaspersky Anti-Virus verifica automaticamente la presenza di nuovi aggiornamenti sui server di Kaspersky Lab. Se il server contiene un nuovo insieme di aggiornamenti, Kaspersky Anti-Virus li scaricherà e li installerà automaticamente.

Se i database inclusi nel pacchetto di installazione sono obsoleti, le dimensioni del pacchetto di aggiornamento possono essere piuttosto grandi e aumentare ulteriormente il traffico in Internet (fino a diverse decine di MB).

Per garantire una protezione completa del computer, si consiglia di aggiornare Kaspersky Anti-Virus immediatamente dopo l'installazione.

➡ *Per aggiornare Kaspersky Anti-Virus autonomamente, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Premere il pulsante **Avvia aggiornamento**.

GESTIONE DELLE LICENZE

Per poter funzionare, Kaspersky Anti-Virus richiede una licenza che viene fornita all'acquisto del prodotto. Tale licenza consente di utilizzare il prodotto non appena questo viene attivato.

A meno che non sia stata attivata una versione di prova, senza una licenza Kaspersky Anti-Virus viene eseguito nella modalità che consente di scaricare un solo aggiornamento. Al termine del periodo di prova, la versione di prova di Kaspersky Anti-Virus attivata non funziona più.

Se è stata attivata una versione di prova dell'applicazione, alla sua scadenza Kaspersky Anti-Virus non verrà avviato.

Quando la licenza commerciale scade, l'applicazione continua a funzionare, ma non sarà possibile aggiornare i database. Resta comunque possibile eseguire la scansione del computer per identificare la presenza di eventuali virus e utilizzare i componenti di protezione, ma solo attraverso i database aggiornati fino alla scadenza della licenza. Ciò significa che la protezione dai virus diffusi dopo la scadenza della licenza del programma non può essere garantita.

Per evitare di infettare il computer con nuovi virus, si consiglia di rinnovare la licenza di Kaspersky Anti-Virus. Due settimane prima della scadenza della licenza, verrà visualizzato un avviso. Durante un determinato periodo, a ogni avvio del programma verrà visualizzato un messaggio corrispondente.

Nella sezione **Licenza** della finestra principale di Kaspersky Anti-Virus sono contenute informazioni generali sulla licenza attualmente in uso (la licenza attiva e quelle aggiuntive, se installate): tipo di licenza (completa, di prova, beta), numero massimo di host, data di scadenza della licenza e numero di giorni mancanti alla data di scadenza. Per ulteriori dettagli sulla licenza, fare clic sul collegamento con il tipo di licenza attualmente in uso.

Per visualizzare il contratto di licenza dell'applicazione, fare clic sul pulsante **Visualizza il Contratto di licenza con l'utente finale**.

Per rimuovere la licenza, fare clic sul pulsante **Aggiungi** / **Elimina** e seguire tutte le istruzioni della procedura guidata successivamente visualizzata.

Kaspersky Lab propone offerte speciali per il rinnovo della licenza dei prodotti. Verificare sul sito Web di Kaspersky Lab la presenza di eventuali offerte speciali.

➡ *Per acquistare o rinnovare una licenza, eseguire le seguenti operazioni:*

1. Acquistare un nuovo file chiave o un codice di attivazione. Premere i pulsanti **Acquista licenza** (se l'applicazione non è stata attivata) o **Rinnovo licenza**. Nella pagina Web visualizzata sono contenute informazioni dettagliate sui termini di acquisto della chiave dall'eStore di Kaspersky Lab o da distributori autorizzati. Se si effettua un acquisto online, una volta eseguito il pagamento verrà inviato un file chiave o un codice di attivazione via e-mail all'indirizzo specificato nel modulo d'ordine.

2. Attivare l'applicazione. Utilizzare il pulsante **Aggiungi /Elimina** nella sezione **Licenza** della finestra principale dell'applicazione oppure usare il comando **Attiva** dal menu di scelta rapida. Verrà eseguita l'attivazione guidata.

GESTIONE DELLA PROTEZIONE

I problemi nella protezione del computer vengono indicati dallo stato della protezione del computer (vedere la sezione "Finestra principale dell'applicazione" a pag.41), che viene visualizzato dai cambiamenti dei colori dell'icona di stato della protezione e del pannello in cui si trova. Se il sistema di protezione presenta problemi, si consiglia di risolverli.

Fig. 1. Stato attuale della protezione del computer

È possibile visualizzare l'elenco dei problemi che si sono verificati, la descrizione e le soluzioni possibili, mediante l'impostazione guidata protezione (vedere figura in basso) che è possibile attivare facendo clic sul collegamento **Ripara** (vedere figura in alto).

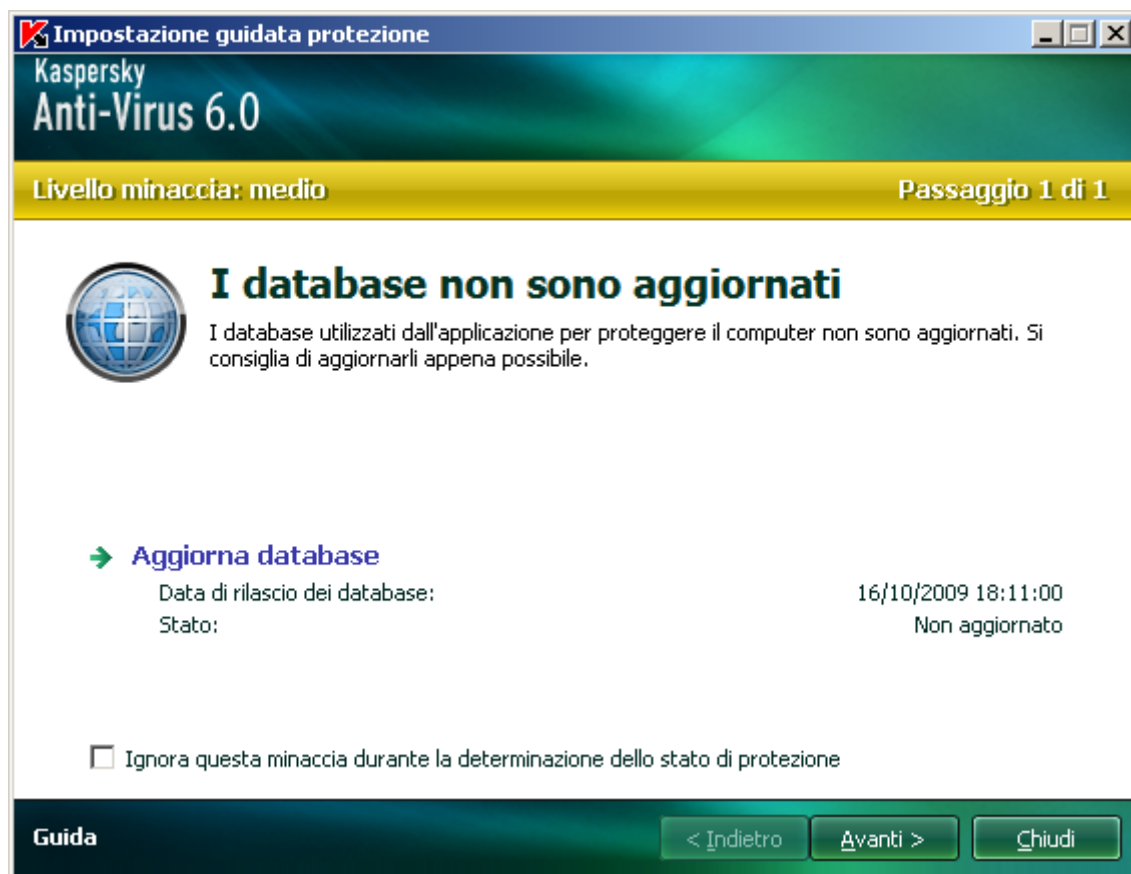



Fig. 2. Risoluzione dei problemi di protezione

Viene visualizzato l'elenco dei problemi correnti. I problemi vengono ordinati in base al livello di criticità: innanzitutto, i problemi più critici, ovvero quelli visualizzati con l'icona di stato rossa, quindi quelli meno importanti, ovvero con l'icona di stato gialla, infine i messaggi informativi. Per ciascun problema viene fornita una descrizione dettagliata e sono disponibili le azioni seguenti:

- *Eliminazione immediata*. Utilizzando i collegamenti appropriati, è possibile passare alla risoluzione del problema, ovvero l'azione consigliata.

- *Rimanda l'eliminazione*. Se non si riesce a eliminare il problema immediatamente, è possibile rimandare questa azione. Selezionare la casella **Ignora questa minaccia durante la determinazione dello stato di protezione** affinché la minaccia non abbia conseguenze sullo stato di protezione corrente.

  Si noti che questa opzione non è disponibile per i problemi più seri. Tali problemi comprendono ad esempio gli oggetti dannosi non disinfettati, il blocco di uno o più componenti o il danneggiamento dei file dell'applicazione. Tale tipo di problemi devono essere eliminati nella maniera più rapida possibile.

SOSPENSIONE DELLA PROTEZIONE

La sospensione della protezione comporta la disabilitazione temporanea di tutti i componenti di protezione che monitorano i file del computer, la posta in entrata e in uscita, il traffico Internet, il comportamento delle applicazioni, le funzioni Anti-Hacker e Anti-Spam.

Per sospendere Kaspersky Anti-Virus, eseguire le seguenti operazioni:

1. Nel menu di scelta rapida dell'applicazione, selezionare la voce **Sospendi protezione**.

2. Nella finestra **Sospendi protezione** visualizzata, dalle opzioni suggerite selezionare il periodo di tempo in cui si desidera che la protezione sia attivata.

ELIMINAZIONE DEI PROBLEMI. ASSISTENZA TECNICA UTENTE

Se i problemi si verificano durante il funzionamento di Kaspersky Anti-Virus, per trovare la soluzione al problema si consiglia in primo luogo di consultare la Guida in linea. In secondo luogo, si consiglia di consultare la Knowledge Base di Kaspersky Lab (http://support.kaspersky.com). La *Knowledge Base* è una sezione apposita del sito Web dell'Assistenza tecnica di Kaspersky Lab che contiene i consigli per i prodotti Kaspersky Lab e le risposte alle domande più frequenti. Si può provare a trovare una risposta alla propria domanda o una soluzione al proprio problema utilizzando questa risorsa.

Per utilizzare la Knowledge Base, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Servizio di assistenza tecnica**.

Un'altra risorsa per ottenere informazioni sull'uso dell'applicazione è il forum degli utenti di Kaspersky Lab. Si tratta anche in questo caso di una sezione distinta del sito Web dell'Assistenza tecnica che contiene domande, feedback e richieste degli utenti. È possibile visualizzare gli argomenti principali, lasciare un proprio feedback o trovare risposte alle proprie domande.

Per aprire il forum degli utenti, eseguire le seguenti operazioni:

1. Aprire la finestra principaledell'applicazione.
2. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Forum utenti**.

Se non si trova una soluzione al problema nella Guida, nella Knowledge Base o nel Forum degli utenti, si consiglia di contattare l'Assistenza tecnica di Kaspersky Lab.

CREAZIONE DI UN FILE DI TRACCIA

Dopo l'installazione di Kaspersky Anti-Virus, possono verificarsi problemi nel sistema operativo o nel funzionamento di singole applicazioni. La causa più probabile è un conflitto tra l'applicazione e il software installato nel computer o con i driver dei componenti del computer. Per consentire agli specialisti di Kaspersky Lab di risolvere il problema, potrebbe essere necessario creare un file di traccia.

Per creare il file di traccia:

1. Aprire la finestra principaledell'applicazione.
2. Nella parte inferiore della finestra, fare clic sul collegamento **Assistenza**.
3. Nella finestra **Assistenza** visualizzata, fare clic sul collegamento **Tracce**.
4. Nella finestra **Informazioni per il servizio di assistenza tecnica** visualizzata, utilizzare l'elenco a discesa della sezione **Tracce** per selezionare il livello di traccia. Tale livello deve essere impostato in base alle indicazioni dello specialista dell'Assistenza tecnica. In assenza di istruzioni da parte dell'Assistenza tecnica, si consiglia di utilizzare il livello di traccia **500**.
5. Per iniziare il processo di creazione di una traccia, fare clic sul pulsante **Attiva**.

6. Riprodurre la situazione che ha causato il problema.

7. Per arrestare il processo di creazione della traccia, cliccare sul pulsante **Disattiva**.

CONFIGURAZIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE

La finestra delle impostazioni dell'applicazione (vedere a pag. 147), accessibile dalla finestra principale premendo il pulsante **Impostazioni**, consente di accedere rapidamente alle impostazioni i Kaspersky Anti-Virus 6.0.

RAPPORTI SUL FUNZIONAMENTO DELL'APPLICAZIONE. FILE DI DATI

Il funzionamento di ciascun componente di Kaspersky Anti-Virus e le prestazioni di ciascuna scansione anti-virus e attività di aggiornamento vengono registrate in un rapporto (vedere a pag. 169). Per visualizzare i rapporti, utilizzare il pulsante **Rapporto** che si trova in basso a destra nella finestra principale.

Gli oggetti messi in quarantena (vedere a pag. 170) o posizionati nel backup (vedere a pag. 171) da Kaspersky Anti-Virus, sono denominati *file dati dell'applicazione*. Premendo il pulsante **Rilevati**, viene aperta la finestra **Archiviazione**, in cui è possibile elaborare questi oggetti, se necessario.

INTERFACCIA DELL'APPLICAZIONE

Kaspersky Anti-Virus presenta un'interfaccia di facile utilizzo. In questo capitolo vengono messe in risalto le funzioni di base.

Oltre all'interfaccia di base, l'applicazione dispone di componenti di espansione (plugin) integrati nelle applicazione Microsoft Office Outlook (scansione anti-virus e scansione anti-spam), Microsoft Outlook Express (Windows Mail), The Bat! (scansione anti-virus e scansione anti-spam), Microsoft Internet Explorer ed Esplora risorse. I plugin espandono le funzioni di questi programmi rendendo disponibile la gestione e le impostazioni di Kaspersky Anti-Virus all'interno delle rispettive interfacce.

IN QUESTA SEZIONE

Icona dell'area di notifica della barra delle applicazioni ....

Menu di scelta rapida ....

Finestra principale dell'applicazione ....

Notifiche ....

Finestra delle impostazioni dell'applicazione ....

VEDERE ANCHE

Scansione della posta elettronica in Microsoft Office Outlook.........................

Scansione della posta elettronica nel plug-in The Bat!.....................................

Configurazione dell'elaborazione della posta spam in Microsoft Office Outlook..

Configurazione dell'elaborazione della posta spam in Microsoft Outlook Express (Windows Mail).........................

Configurazione dell'elaborazione della posta spam in The Bat! ....

ICONA DELL'AREA DI NOTIFICA DELLA BARRA DELLE APPLICAZIONI

Subito dopo aver installato Kaspersky Anti-Virus, la relativa icona viene visualizzata nell'area di notifica della barra delle applicazioni di Microsoft Windows.

Questa icona è un indicatore del funzionamento dell'applicazione. Riflette inoltre lo stato della protezione e visualizza numerose funzioni di base eseguite dall'applicazione.

Se l'icona è attiva (è colorata), significa che la protezione è abilitata sul computer. Se l'icona è inattiva (grigia), significa che tutti i componenti di protezione (a pag. 17) sono disabilitati.

L'icona di Kaspersky Anti-Virus cambia in funzione dell'operazione eseguita:

– scansione della posta elettronica in corso.

– scansione del traffico HTTP in corso.

– scansione in corso di un file che l'utente o un programma stanno aprendo, salvando o eseguendo.

– aggiornamento in corso del database e del modulo di Kaspersky Anti-Virus.

– è necessario riavviare il computer per applicare gli aggiornamenti.

– si è verificato un errore nel funzionamento di alcuni componenti di Kaspersky Anti-Virus.

L'icona consente inoltre di accedere ai componenti di base dell'interfaccia dell'applicazione: il menu di scelta rapida e la finestra principale.

Per aprire il menu di scelta rapida, fare clic con il pulsante destro del mouse sull'icona dell'applicazione.

Per aprire la finestra principale di Kaspersky Anti-Virus**,** fare clic sull'icona dell'applicazione.

MENU DI SCELTA RAPIDA

Il menu di scelta rapida consente di eseguire le attività di protezione di base e contiene le seguenti voci:

- **Scansione completa –** consente di avviare una scansione completa (vedere a pag. 124) del computer alla ricerca di oggetti dannosi. Durante l'operazione vengono esaminati gli oggetti di tutte le unità, inclusi i supporti rimovibili.
- **Scansione –** consente di selezionare gli oggetti e avviare la scansione anti-virus. Per impostazione predefinita, l'elenco contiene diversi file, quali la cartella **Documenti**, gli oggetti di avvio, i database della posta elettronica, tutte le unità disco del computer e così via. È possibile ingrandire l'elenco, selezionare altri oggetti e avviare la scansione anti-virus.
- **Aggiornamento** – avvia gli aggiornamenti (vedere a pag. 135) dei moduli e dei database di Kaspersky Anti-Virus e li installa sul computer.
- **Monitor rete** – consente di visualizzare l'elenco (vedere a pag. 100) delle connessioni di rete stabilite, delle porte aperte e del traffico.
- **Attiva** – attiva l'applicazione (vedere a pag. 28). Per diventare un utente registrato con accesso alle piene funzionalità dell'applicazione e all'assistenza tecnica, è necessario attivare la propria versione di Kaspersky Anti-Virus. Questa voce di menu è disponibile solo se l'applicazione non è attivata.
- **Impostazioni** – consente di visualizzare e modificare le impostazioni (vedere a pag. 147) di Kaspersky Anti-Virus.
- **Kaspersky Anti-Virus** – apre la finestra principale dell'applicazione (vedere a pag. 41).
- **Sospendi protezione / Riprendi protezione** – disabilita o abilita temporaneamente i componenti di protezione (vedere a pag. 17). Questa voce di menu non ha effetto sull'esecuzione della scansione anti-virus o sugli aggiornamenti dell'applicazione.
- **Disabilita criteri / Abilita criteri -** disabilita o abilita temporaneamente i criteri mediante il Kaspersky Administration Kit, durante il funzionamento dell'applicazione. Questa voce di menu consente la rimozione del computer dall'ambito operativo di criteri e attività di gruppo. Questa opportunità viene gestita tramite password. La voce di menu viene visualizzata solo se è stata impostata una password.
- **Informazioni su** – visualizza la finestra contenente le informazioni sull'applicazione.

- **Esci** – chiude Kaspersky Anti-Virus (scegliendo questa opzione, l'applicazione viene rimossa dalla RAM del computer).

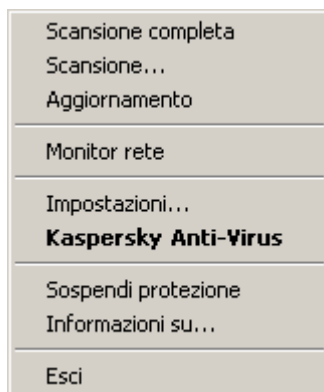



Fig. 3. Menu di scelta rapida

Se è in esecuzione un'attività di scansione anti-virus, il nome di quest'ultima verrà visualizzato nel menu di scelta rapida con l'indicazione dell'avanzamento in percentuale. Dopo la selezione di un'attività, nella finestra dei rapporti è possibile visualizzare i risultati delle prestazioni correnti.

FINESTRA PRINCIPALE DELL'APPLICAZIONE

La finestra principale dell'applicazione può essere divisa in tre parti:

- La parte superiore della finestra indica l'attuale stato di protezione del computer.

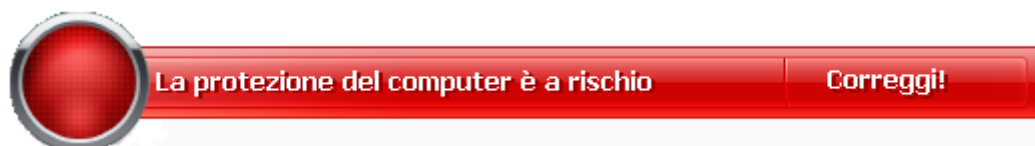



Fig. 4. Stato attuale della protezione del computer

Vi sono tre valori possibili dello stato di protezione: ciascuno di essi viene indicato da un determinato colore, analogamente a un semaforo. Il verde indica che la protezione del computer è di livello adeguato, il giallo ed il rosso evidenziano la presenza di minacce alla protezione nella configurazione del sistema o nel funzionamento di Kaspersky Anti-Virus. Oltre ai programmi dannosi, anche il mancato aggiornamento dei database dell'applicazione obsoleti, la disabilitazione di componenti di protezione e la selezione di impostazioni di protezione minime vengono considerate minacce.

Le minacce alla protezione devono essere eliminate non appena compaiono. Per ottenere informazioni dettagliate su di esse ed eliminarle rapidamente, utilizzare il collegamento **Ripara** (vedere figura in alto).

- La parte sinistra della finestra consente di accedere rapidamente a qualsiasi funzione dell'applicazione, incluse le attività di scansione anti-virus, di aggiornamento e così via.

Fig. 5. Parte sinistra della finestra principale

- La parte destra della finestra contiene informazioni sulla funzione dell'applicazione selezionata nella parte sinistra, consente di configurare tali funzioni e offre strumenti per eseguire attività di scansione anti-virus, scaricare aggiornamenti e così via.

Fig. 6. Parte destra della finestra principale

È inoltre possibile utilizzare:

- Il pulsante **Impostazioni** – per aprire la finestra delle impostazioni (vedere a pag. 147);
- Il collegamento **Guida** – per aprire la Guida di Kaspersky Anti-Virus;
- Il pulsante **Rilevati** – per utilizzare i file di dati dell'applicazione (vedere a pag. 168);
- Il pulsante **Rapporto** – per aprire i rapporti dei componenti (vedere a pag. 169) dell'applicazione;
- Il collegamento **Supporto** – per aprire la finestra contenente le informazioni sul sistema e i collegamenti alle risorse informative di Kaspersky Lab (vedere a pag. 37) (sito del servizio dell'assistenza tecnica, forum).

NOTIFICHE

Se durante l'esecuzione di Kaspersky Anti-Virus si verificano degli eventi, sullo schermo vengono visualizzate notifiche speciali sotto forma di messaggi a comparsa al di sopra dell'icona dell'applicazione sulla barra delle applicazioni di Microsoft Windows.

A seconda della criticità dell'evento per la protezione del computer, potrebbero essere visualizzati i tipi di notifica seguenti:

- **Allarme**. Si è verificato un evento critico, ad esempio è stato rilevato un virus o un'attività pericolosa nel sistema. È necessario decidere subito come affrontare la minaccia. Questo tipo di notifica è visualizzata in rosso.

- **Attenzione**. Si è verificato un evento potenzialmente pericoloso. Ad esempio, nel sistema sono stati rilevati file potenzialmente infetti o un'attività sospetta. È necessario stabilire quanto è pericoloso l'evento in questione. Questo tipo di notifica è visualizzata in giallo.
- **Informazioni**. Questa notifica fornisce informazioni su eventi non critici. Questo tipo, ad esempio, include le notifiche relative al funzionamento del componente Anti-Hacker. Le notifiche di priorità minore hanno il codice colore verde.

VEDERE ANCHE

Tipi di notifiche 189

FINESTRA DELLE IMPOSTAZIONI DELL'APPLICAZIONE

È possibile aprire la finestra delle impostazioni di Kaspersky Anti-Virus a partire dalla finestra principale oppure tramite il menu di scelta rapida. Per effettuare questa operazione, premere il pulsante **Impostazioni** nella parte superiore della finestra principale oppure selezionare l'opzione appropriata dal menu di scelta rapida dell'applicazione.

La finestra delle impostazioni si compone di due parti:

- la parte sinistra consente di accedere ai componenti di Kaspersky Anti-Virus, alle attività di scansione anti-virus, alle attività di aggiornamento e così via.
- la parte destra della finestra contiene un elenco di impostazioni relative, ad esempio, al componente e all'attività selezionati nella parte sinistra della finestra.

VEDERE ANCHE

Configurazione delle impostazioni dell'applicazione 147

ANTI-VIRUS FILE

Anti-Virus File impedisce l'infezione del file system del computer. Tale strumento viene caricato all'avvio del sistema operativo ed eseguito nella RAM del computer. Esamina tutti i file che vengono aperti, salvati o eseguiti.

Per impostazione predefinita, mediante il componente Anti-Virus File esegue solo la scansione dei file nuovi o modificati. Una serie di impostazioni, denominata livello di protezione, determina la modalità di scansione dei file. Se il componente Anti-Virus File rileva una minaccia, eseguirà l'azione preimpostata.

Il livello di protezione dei file e della memoria sul computer è determinato dalle combinazioni di impostazioni seguenti:

- impostazioni dell'ambito di protezione;
- impostazioni che definiscono il metodo di scansione utilizzato;
- impostazioni che definiscono la scansione di file composti (così come la scansione di file composti di grandi dimensioni);
- impostazioni che definiscono la modalità di scansione;
- impostazioni utilizzate per sospendere il funzionamento del componente (in base alla pianificazione, durante il funzionamento di applicazioni selezionate).

Per modificare le impostazioni di Anti-Virus File:

1. Aprire la finestra principaledell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, apportare le modifiche desiderate alle impostazioni del componente.

IN QUESTA SEZIONE

Algoritmo di funzionamento del componente 46

Modifica del livello di protezione 47

Modifica delle azioni da eseguire sugli oggetti rilevati 48

Creazione di un ambito di protezione 49

Utilizzo dell'analisi euristica 50

Ottimizzazione della scansione 50

Scansione dei file compositi 51

Scansione di file composti di grandi dimensioni 51

Modifica della modalità di scansione 52

Tecnologia di scansione 52

Sospensione del componente: creazione di una pianificazione 53

Sospensione del componente: creazione di un elenco di applicazioni 53

Ripristino delle impostazioni di protezione predefinite 54

Statistiche di Anti-Virus File 54

Trattamento posticipato degli oggetti 55

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Il componente *Anti-Virus File* viene caricato all'avvio del sistema operativo, viene eseguito nella memoria del computer ed esamina tutti i file che vengono aperti, salvati o eseguiti.

Per impostazione predefinita, Anti-Virus File esamina solo i file nuovi o modificati, ovvero i file che sono stati aggiunti o modificati dall'ultima scansione. I file vengono esaminati secondo il seguente algoritmo:

1. Il componente intercetta gli accessi a ciascun file da parte dell'utente o di qualsiasi programma.

2. Anti-Virus File esegue la scansione dei database iChecker e iSwift alla ricerca di informazioni sul file individuato e determina se è necessario eseguire la scansione del file, in base alle informazioni recuperate.

La scansione include i seguenti passaggi:

- Il file viene esaminato alla ricerca di virus. Gli oggetti vengono rilevati mediante comparazione con i database dell'applicazione. Il database contiene le descrizioni di tutti i programmi dannosi e le minacce attualmente noti, nonché i metodi per elaborarli.

- Al termine dell'analisi, è possibile eseguire una delle azioni di Kaspersky Anti-Virus seguenti:

  a. Se nel file viene rilevato codice dannoso, File Anti-Virus blocca il file, ne crea una copia di *backup* e tenta di disinfettarlo. Al termine della disinfezione del file, quest'ultimo diventa utilizzabile da parte dell'utente. Se la disinfezione non riesce, il file viene eliminato.

b. Se viene rilevato codice potenzialmente dannoso, senza alcuna garanzia dell'effettiva pericolosità, il file viene comunque disinfettato e quindi inviato in un'area di archiviazione speciale denominata *Quarantena*.

c. Se nel file non viene rilevato codice dannoso, esso viene immediatamente ripristinato.

Se viene rilavato un file infetto o potenzialmente infetto, verrà visualizzata una notifica. È necessario reagire alla notifica sottoponendo il file a ulteriore elaborazione:

- mettere in quarantena l'oggetto, in modo da poter esaminare ed elaborare successivamente la nuova minaccia con i database aggiornati;
- eliminare l'oggetto;
- ignorare la situazione, se si ritiene che l'oggetto non sia dannoso.

VEDERE ANCHE

Anti-Virus File 45

MODIFICA DEL LIVELLO DI PROTEZIONE

Il livello di protezione è definito come configurazione preimpostata delle impostazioni del componente Anti-Virus File. Gli specialisti di Kaspersky Lab distinguono tre livelli di protezione. Per decidere quale livello selezionare, l'utente deve considerare le condizioni operative e la situazione corrente.

- Se il computer ha una grande possibilità di infettarsi, è necessario selezionare il livello di protezione alto.
- Il livello consigliato garantisce un equilibrio ottimale tra efficienza e protezione ed è adatto nella maggior parte dei casi.
- Se si lavora in un ambiente protetto, ad esempio in una rete aziendale con una gestione della protezione centralizzata, o con applicazioni dall'alto consumo di risorse, si consiglia di selezionare il livello di protezione basso.

Prima di abilitarlo, è consigliabile eseguire la scansione completa del computer con un livello di protezione alto.

Se nessuno dei livelli preimpostati soddisfa le proprie esigenze, è possibile configurare manualmente le impostazioni di Anti-Virus File. Di conseguenza, il nome del livello di protezione cambierà in **Personalizzato**. Per ripristinare le impostazioni predefinite del componente, selezionare uno dei livelli di protezione preimpostati.

Per modificare il livello di protezione selezionato del componente Anti-Virus File, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.
4. Selezionare il livello di protezione desiderato nella finestra visualizzata.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

Come risultato della scansione, Anti-Virus File assegna uno degli stati seguenti agli oggetti rilevati:

- programma dannoso, ad esempio nel caso di un *virus* o di un *Trojan*;
- *potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che l'applicazione ha rilevato nel file una sequenza di codice di un virus sconosciuto o un codice modificato di un virus conosciuto.

Se, durante la scansione anti-virus di un file, Kaspersky Anti-Virus individua oggetti infetti o potenzialmente infetti, le azioni successive eseguite da Anti-Virus File dipendono dallo stato degli oggetti e dall'azione selezionata.

Per impostazione predefinita, tutti i file infetti sono sottoposti a disinfezione e tutti quelli potenzialmente infetti vengono messi in quarantena.

Tutte le azioni possibili sono mostrate nella tabella seguente.

SE L'AZIONE SCELTA È	SE VIENE RILEVATO UN OGGETTO PERICOLOSO
Richiedi intervento utente	Anti-Virus File mostra un messaggio di avviso contenente informazioni su quale programma dannoso abbia infettato o possa infettare il file e offre una serie di possibili azioni. Le azioni possono variare in base allo stato dell'oggetto.
Blocca l'accesso	Anti-Virus File blocca l'accesso all'oggetto. Le informazioni rilevanti vengono registrate nel rapporto. In un secondo momento sarà possibile provare a disinfettare l'oggetto.
Blocca l'accesso **Disinfetta**	Anti-Virus File blocca l'accesso all'oggetto e tenta di disinfettarlo. Se la disinfezione riesce, viene ripristinato al suo uso normale. Se il tentativo di disinfezione dell'oggetto non riesce, quest'ultimo verrà bloccato (se non è possibile disinfettare l'oggetto) oppure gli verrà assegnato lo stato di *potenzialmente infetto* (se l'oggetto è considerato sospetto) e verrà messo in Quarantena. Le informazioni rilevanti vengono registrate nel rapporto. In un secondo momento sarà possibile provare a disinfettare l'oggetto.
Blocca l'accesso **Disinfetta** **Elimina se la disinfezione non riesce**	Anti-Virus File blocca l'accesso all'oggetto e tenta di disinfettarlo. Se la disinfezione riesce, viene ripristinato al suo uso normale. Se la disinfezione non riesce, l'oggetto viene eliminato. Una copia dell'oggetto viene archiviata nel Backup.
Blocca l'accesso **Disinfetta** **Elimina**	Anti-Virus File blocca l'accesso all'oggetto e lo elimina.

Prima di provare a disinfettare o eliminare un oggetto infetto, Kaspersky Anti-Virus ne crea una copia di backup e la archivia nel Backup per consentirne il ripristino o la disinfezione in un secondo momento.

Per modificare l'azione da eseguire sugli oggetti rilevati, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.

4. Selezionare l'azione desiderata nella finestra che viene visualizzata.

CREAZIONE DI UN AMBITO DI PROTEZIONE

Un ámbito di protezione definisce, oltre alla posizione degli oggetti da esaminare, anche il tipo di file da esaminare. Per impostazione predefinita, Kaspersky Anti-Virus esegue solo la scansione dei aperti file potenzialmente infettabili in qualsiasi disco rigido, unità di rete o unità rimovibile.

È possibile espandere o restringere l'ambito di protezione aggiungendo / rimuovendo gli oggetti da esaminare oppure modificando i tipi di file da esaminare. Ad esempio, si desidera eseguire solo la scansione dei file .exe contenuti nelle unità di rete. è necessario agire con cautela per far sì che il computer non venga esposto alla minaccia di infezioni causate dalla limitazione dell'ambito di protezione.

Quando si selezionano i tipi di file, si tenga presente quanto segue:

- Esistono diversi formati di file con un livello di rischio discretamente basso di contenere codice dannoso che potrebbe essere attivato in seguito (ad esempio i file *.txt*). Altri formati, al contrario, contengono o possono contenere codice eseguibile, ad esempio i formati *.exe*, *.dll*, *.doc*. e il rischio di attivazione di codice dannoso al loro interno è estremamente alto.

- È importante ricordare che un utente malintenzionato può inviare un virus al computer in un file con estensione *txt* che in realtà è un file eseguibile rinominato come *txt*. Selezionando l'opzione **Scansione file per estensione**, tale file viene escluso dalla scansione. Selezionando l'impostazione **Scansione file per formato**, Anti-Virus File analizza l'intestazione del file indipendentemente dall'estensione, rileva se si tratta di un file *.exe*, quindi esegue la scansione anti-virus.

Quando si specificano i tipi di file da esaminare, vengono definiti il formato e le dimensioni dei file e le unità su cui verrà eseguita la scansione anti-virus per l'apertura, l'esecuzione o il salvataggio di tali file.

Per facilitare la configurazione, tutti i file vengono suddivisi in due gruppi: *semplici* e *composti*. I file semplici non contengono oggetti (ad esempio i file .txt). I file composti possono contenere diversi oggetti, ciascuno dei quali, a sua volta, può presentare diversi livelli nidificati. Tali oggetti possono essere archivi, file contenenti macro, fogli di calcolo, e-mail con allegati e così via.

È opportuno ricordare che Anti-Virus File eseguirà solo la scansione dei file inclusi nell'ambito di protezione creato. I file che non sono inclusi risulteranno disponibili all'uso senza scansione. Ciò aumenta il rischio di infezione del computer.

Per modificare l'elenco di scansione degli oggetti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nelle finestra visualizzata, all'interno della scheda **Generale**, nella sezione **Ambito della protezione**, premere il pulsante **Aggiungi**.
6. Nella finestra **Selezionare oggetto da analizzare**, selezionare un oggetto, quindi premere il pulsante **Aggiungi**. Premere il pulsante **OK** dopo aver aggiunto tutti gli oggetti necessari.
7. Per escludere un oggetto dall'elenco di oggetti da esaminare, deselezionare la relativa casella.

Per modificare il tipo di oggetto esaminato:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.

4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.

5. Nella finestra visualizzata, selezionare le impostazioni necessarie all'interno della scheda **Generale**, nella sezione **Tipi di file**.

UTILIZZO DELL'ANALISI EURISTICA

Gli oggetti vengono esaminati utilizzando database che contengono le descrizioni di tutti i malware noti e i metodi di disinfezione corrispondenti. Kaspersky Anti-Virus confronta ogni oggetto esaminato con le voci del database per determinare se si tratta di un oggetto dannoso e, in tal caso, identifica la classe di malware cui appartiene. Questo approccio è noto come *analisi della firma* e viene sempre utilizzato per impostazione predefinita.

Ogni giorno vengono creati nuovi oggetti dannosi. Non tutti sono descritti nei database e possono quindi essere rilevati solo attraverso l'analisi euristica. Questo metodo presuppone l'analisi delle azioni eseguite da un oggetto all'interno del sistema. Se tali azioni sono tipiche di oggetti dannosi, è probabile che l'oggetto venga classificato come dannoso o sospetto. In questo modo è possibile rilevare le nuove minacce prima ancora che queste vengano studiate dagli analisti anti-virus.

Inoltre, è possibile impostare il livello di dettaglio delle scansioni. Questo livello definisce un equilibrio tra il livello di dettaglio delle ricerche di nuove minacce, il carico sulle risorse del sistema operativo e il tempo richiesto per la scansione. Maggiore è il livello di dettaglio, più risorse saranno necessarie e maggiore sarà la durata della scansione.

➡ *Per utilizzare l'analisi euristica e impostare il livello di dettaglio delle scansioni:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.

4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.

5. Nella finestra visualizzata, all'interno della scheda **Prestazioni**, nella sezione **Metodi di scansione**, selezionare la casella ☑ **Analisi euristica** e impostare il livello di dettaglio della scansione.

OTTIMIZZAZIONE DELLA SCANSIONE

Per ridurre la durata delle scansioni e per aumentare la velocità di Kaspersky Anti-Virus, è possibile scegliere di sottoporre a scansione solo i file nuovi e i file modificati dopo l'ultima analisi. Questa modalità si estende ai file semplici e a quelli compositi.

➡ *Per sottoporre a scansione solo i file nuovi e quelli modificati dall'ultima scansione:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.

4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.

5. Nella finestra visualizzata, all'interno della scheda **Prestazioni** selezionare la casella ☑ **Esamina solo file nuovi e modificati**.

SCANSIONE DEI FILE COMPOSITI

Un metodo comune di nascondere i virus è quello di incorporarli nei file composti, come gli archivi, i database e così via. Per rilevare i virus nascosti in questa maniera, il file composto deve essere decompresso e ciò può diminuire in maniera significativa la velocità della scansione.

I pacchetti di installazione e i file contenenti oggetti OLE vengono eseguiti all'apertura, risultando quindi più pericolosi degli archivi. Per proteggere il computer contro l'esecuzione di codice dannoso e, allo stesso tempo, aumentare la velocità di scansione, è necessario disabilitare le scansioni degli archivi e abilitare le scansioni per questo tipo di file.

Se un file contenente un oggetto OLE è un archivio, verrà sottoposto a scansione durante la decompressione. È possibile abilitare la scansione di archivi per analizzare file contenenti oggetti OLE incorporati prima della loro decompressione. Tuttavia, questa operazione comporterà una significativa diminuzione della velocità di scansione.

Per impostazione predefinita, Kaspersky Anti-Virus esamina esclusivamente gli oggetti OLE incorporati.

➡ *Per modificare l'elenco dei file compositi esaminati:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Prestazioni**, nella sezione **Scansione di file composti**, selezionare le caselle dei tipi di file composti da esaminare.

SCANSIONE DI FILE COMPOSTI DI GRANDI DIMENSIONI

Durante la scansione di file compositi di grandi dimensioni, la decompressione preliminare può richiedere molto tempo. È possibile ridurre questo tempo solo se si esegue la scansione dei file in background. Se durante l'utilizzo di questi file è stato rilevato un oggetto dannoso, viene visualizzato un messaggio di notifica.

Per accedere più rapidamente ai file composti, disabilitare la decompressione dei file di dimensioni superiori a quelle specificate. Quando i file vengono estratti da un archivio, vengono sempre sottoposti a scansione.

➡ *Se si desidera abilitare la decompressione in background di file di grandi dimensioni, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Prestazioni**, nella sezione **Scansione di file composti**, premere il pulsante **Avanzate**.
6. Nella finestra **File composti**, selezionare la casella ☑ **Estrai i file composti in background**, quindi specificare il valore minimo delle dimensione del file nel campo sottostante.

➡ *Se non si desidera abilitare la decompressione in background di file di grandi dimensioni, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.

4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.

5. Nella finestra visualizzata, all'interno della scheda **Prestazioni**, nella sezione **Scansione di file composti**, premere il pulsante **Avanzate**.

6. Nella finestra **File composti**, selezionare la casella ☑ **Non decomprimere file composti di grandi dimensioni**, quindi specificare il valore massimo delle dimensione del file nel campo sottostante.

MODIFICA DELLA MODALITÀ DI SCANSIONE

Per modalità di scansione si intende la condizione che attiva il funzionamento del componente Anti-Virus File. Per impostazione predefinita, l'applicazione utilizza la modalità Smart che determina se l'oggetto debba essere esaminato sulla base delle azioni eseguite su di esso. Ad esempio, quando si lavora con un documento Microsoft Office, il file viene sottoposto a scansione quando viene aperto per la prima e chiuso per l'ultima volta. Le operazioni intermedie che lo sovrascrivono non determinano la scansione del file.

La modalità di scansione degli oggetti può essere modificata. La selezione della modalità dipende dai file con i quali si lavora più spesso.

➧ *Per modificare la modalità di scansione degli oggetti:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.

4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.

5. Nella finestra visualizzata, nella scheda **Avanzate**, sezione **Modalità di scansione**, selezionare la modalità desiderata.

TECNOLOGIA DI SCANSIONE

È inoltre possibile specificare le tecnologie che verranno utilizzate dal componente Anti-Virus File:

- **Tecnologia iChecker**. Questa tecnologia è in grado di aumentare la velocità di scansione escludendo determinati oggetti dalla scansione. Un oggetto viene escluso dalla scansione utilizzando uno speciale algoritmo che prende in considerazione la data di rilascio dei database del programma, la data dell'ultima scansione dell'oggetto e le modifiche alle impostazioni di scansione.

  Ad esempio, si dispone di un file archivio analizzato dall'applicazione che gli ha assegnato lo stato di *non infetto*. Alla scansione successiva, l'applicazione ignorerà questo archivio, a meno che non sia stato modificato o non siano state modificate le impostazioni di scansione. Se la struttura dell'archivio risulta modificata mediante aggiunta di un nuovo oggetto, oppure se le impostazioni di scansione sono state modificate o i database dell'applicazione aggiornati, il programma esaminerà nuovamente l'archivio.

  La tecnologia iChecker presenta alcuni limiti: non funziona con file di grandi dimensioni e si applica solo agli oggetti con una struttura riconosciuta dall'applicazione (ad esempio, .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

- **iSwift**. Questa tecnologia è stata sviluppata a partire dalla tecnologia iChecker per i computer che utilizzano un file system di tipo NTFS. Anche iSwift presenta delle limitazioni: è associata a un percorso di file specifico nel file system e può essere applicata solo a oggetti in NTFS.

Per cambiare tecnologia di scansione degli oggetti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Avanzate**, nella sezione **Tecnologie di scansione**, selezionare il valore necessario.

SOSPENSIONE DEL COMPONENTE: CREAZIONE DI UNA PIANIFICAZIONE

Durante l'esecuzione di determinati programmi che richiedono una considerevole quantità di risorse, è possibile sospendere temporaneamente l'attività del componente Anti-Virus File, consentendo un accesso più rapido agli oggetti. Per ridurre il carico e garantire un accesso rapido agli oggetti, è possibile impostare una pianificazione per la disabilitazione del componente.

Per configurare una pianificazione per sospendere l'attività del componente:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Avanzate**, nella sezione **Sospendi attività**, selezionare la casella ☑ **Programmata**, quindi premere il pulsante **Pianifica**.
6. Nella finestra **Sospendi attività**, specificare l'ora (nel formato 24 ore OO:MM) in cui la protezione verrà sospesa (nei campi **Sospendi l'attività alle** e **Riprendi l'attività alle**).

SOSPENSIONE DEL COMPONENTE: CREAZIONE DI UN ELENCO DI APPLICAZIONI

Durante l'esecuzione di determinati programmi che richiedono una considerevole quantità di risorse, è possibile sospendere temporaneamente l'attività del componente Anti-Virus File, consentendo un accesso più rapido agli oggetti. Per diminuire il carico e garantire un rapido accesso agli oggetti, è possibile configurare le impostazioni per la disabilitazione del componente quando si utilizzano determinate applicazioni.

La configurazione della disabilitazione del componente Anti-Virus File in caso di conflitti con determinate applicazioni rappresenta una misura drastica. In caso di conflitti con il funzionamento del componente, contattare il servizio di assistenza tecnica di Kaspersky Lab (http://support.kaspersky.it/). Gli specialisti dell'Assistenza tecnica sono in grado di aiutare l'utente a risolvere i problemi di funzionamento di Kaspersky Anti-Virus in contemporanea con il software presente nel computer.

Per configurare la sospensione del componente mentre sono in uso le applicazioni specificate, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.

4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.

5. Nella finestra visualizzata, all'interno della scheda **Avanzate**, nella sezione **Sospendi attività**, selezionare la casella **All'avvio dell'applicazione**, quindi premere il pulsante **Seleziona**.

6. Nella finestra **Applicazioni**, creare un elenco di applicazioni la cui esecuzione metterà in sospensione il componente.

RIPRISTINO DELLE IMPOSTAZIONI DI PROTEZIONE PREDEFINITE

Quando si configura Anti-Virus File, è sempre possibile ripristinarne le impostazioni consigliate. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Esse sono raggruppate nel livello di protezione **Consigliato**.

Se, durante la configurazione delle impostazioni di Anti-Virus File, è stato modificato l'elenco di oggetti inclusi nell'area protetta, verrà chiesto se si desidera salvare tale elenco per un utilizzo successivo nel caso di ripristino delle impostazioni iniziali.

Per ripristinare le impostazioni di protezione predefinite e salvare l'elenco modificato degli oggetti inclusi nell'area protetta, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Dal menu di scelta rapida del componente **Anti-Virus File**, selezionare la voce **Impostazioni**.

4. Nella finestra visualizzata, fare clic sul pulsante **Livello predefinito**.

5. Nella finestra **Ripristino delle impostazioni** visualizzata, selezionare la casella **Ambito di protezione**.

STATISTICHE DI ANTI-VIRUS FILE

Tutte le operazioni eseguite dal componente Anti-Virus File vengono registrate in un rapporto speciale che riepiloga i dettagli delle operazioni eseguite dal componente, raggruppate nelle schede seguenti:

- Tutti gli oggetti pericolosi rilevati durante il processo di protezione del file system sono riportati in un elenco contenuto nella scheda *Rilevati*. In tale elenco sono riportati il percorso completo di ciascun oggetto e lo stato assegnatogli da Anti-Virus File. Se il componente ha individuato con successo il programma che ha infettato l'oggetto, a quest'utlimo verrà assegnato lo stato appropriato: ad esempio *virus*, *Trojan* e così via. Se non è possibile stabilire con esattezza il tipo di effetto dannoso, all'oggetto verrà assegnato lo stato *sospetto*. Accanto allo stato viene visualizzata anche l'azione applicata all'oggetto (rilevato, non trovato, disinfettato).

- L'elenco completo degli eventi verificatisi durante l'uso di Anti-Virus File è riportato nella scheda *Eventi*. Gli eventi possono avere i seguenti stati:

  - *informativo* (ad esempio oggetti non elaborati, ignorati in base al tipo);
  - *avviso* (ad esempio se viene rilevato un virus);
  - *commento* (ad esempio se un archivio è protetto da password).

Solitamente, i messaggi informativi sono esclusivamente di riferimento e non rivestono particolare interesse. È possibile disabilitare la visualizzazione dei messaggi informativi. Per effettuare questa operazione, deselezionare la casella **Mostra tutti gli eventi**.

- Le *statistiche* di scansione vengono visualizzate nella scheda relativa. In questa scheda sarà riportato il numero totale di oggetti analizzati, quindi, suddivisi in colonne, verranno visualizzati: il numero di archivi presenti sul numero totale di oggetti analizzati, il numero di oggetti pericolosi, il numero di oggetti disinfettati, il numero di oggetti in quarantena e così via.
- Le impostazioni attive in Anti-Virus File vengono visualizzate nella scheda *Impostazioni*. Utilizzare il collegamento **Modifica impostazioni** per configurare rapidamente il componente.

Per visualizzare informazioni sulle attività del componente, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Rapporto** dal menu di scelta rapida del componente, **Anti-Virus File**.

TRATTAMENTO POSTICIPATO DEGLI OGGETTI

Se è stata selezionata l'azione **Blocca l'accesso** per gli oggetti dannosi, questi ultimi non verranno disinfettati e ne verrà bloccato l'accesso.

Se le azioni selezionate sono state:

Blocca l'accesso

Disinfetta

verranno bloccati anche tutti gli oggetti non disinfettati.

Per ripristinare l'accesso agli oggetti bloccati, è necessario prima effettuare un tentativo di disinfezione. Se un oggetto viene disinfettato con successo, verrà ripristinato per l'uso regolare. Se non è possibile disinfettare l'oggetto, viene offerta la possibilità di *eliminarlo* o *ignorarlo*. In quest'ultimo caso, verrà ripristinato l'accesso al file. Tuttavia, ciò aumenta in maniera significativa il rischio di infezione del computer. Si consiglia vivamente di non ignorare gli oggetti dannosi.

Per accedere agli oggetti bloccati al fine di disinfettarli, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione e fare clic sul collegamento **Rilevati**.
2. Nella finestra visualizzata, all'interno della scheda **Minacce attive**, selezionare gli oggetti necessari, quindi fare clic sul collegamento **Isola tutto**.

ANTI-VIRUS POSTA

Anti-Virus Posta esamina i messaggi di posta elettronica in entrata e in uscita per verificare la presenza di oggetti nocivi. Viene avviato durante il caricamento del sistema operativo, si trova nella RAM ed esamina tutti i messaggi di posta ricevuti tramite i protocolli POP3, SMTP, IMAP, MAPI e NNTP. Inoltre, il componente esegue la scansione del traffico dei client di messaggistica istantanea ICQ e MSN.

Una serie di impostazioni, suddivisa in cosiddetti livelli di protezione, determina la modalità di scansione del traffico. Se il componente Anti-Virus File rileva una minaccia, eseguirà l'azione specificata. Le regole di scansione della posta elettronica sono definite da una serie di impostazioni. Tali impostazioni possono essere suddivise nei gruppi seguenti:

- impostazioni che definiscono il flusso protetto di messaggi;
- impostazioni che definiscono l'utilizzo di metodi di analisi euristica;
- impostazioni che definiscono la scansione di file composti;
- impostazioni che definiscono il filtro di file allegati.

Kaspersky Lab consiglia di evitare di configurare manualmente le impostazioni di Anti-Virus Posta. Nella maggior parte dei casi è sufficiente selezionare un livello di protezione diverso.

Se Anti-Virus Posta è stato disabilitato per qualche motivo, le connessioni al server di posta stabilite prima che sia stato abilitato non verranno monitorate. Inoltre, il traffico dei client di messaggistica immediata non verrà monitorato se la scansione del traffico è stata disabilitata (vedere pagina 60). È necessario riavviare l'applicazione immediatamente dopo l'abilitazione della scansione del traffico oppure dopo l'avvio di Anti-Virus Posta.

Per modificare le impostazioni di Anti-Virus Posta, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Posta**.
4. Nella finestra visualizzata, apportare le modifiche desiderate alle impostazioni del componente.

IN QUESTA SEZIONE

Algoritmo di funzionamento del componente 57

Modifica del livello di protezione 58

Modifica delle azioni da eseguire sugli oggetti rilevati 59

Creazione di un ambito di protezione 60

Selezione del metodo di scansione 60

Scansione della posta elettronica in Microsoft Office Outlook 61

Scansione della posta elettronica nel plug-in The Bat! 62

Utilizzo dell'analisi euristica 62

Scansione dei file compositi 63

Filtro degli allegati 63

Ripristino delle impostazioni di protezione della posta elettronica predefinite 64

Statistiche della protezione della posta elettronica 64

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Anti-Virus Posta viene caricato all'avvio del sistema operativo ed è sempre in esecuzione per esaminare tutta la posta elettronica sui protocolli POP3, SMTP, IMAP, MAPI e NNTP, nonché le connessioni protette (SSL) per POP3 e IMAP.

L'indicatore di funzionamento del componente è l'icona dell'applicazione nell'area di notifica della barra delle applicazioni, che ha un aspetto simile al seguente quando viene eseguita la scansione di un messaggio e-mail.

Per impostazione predefinita, la posta viene protetta nel modo seguente:

1. Ogni messaggio di posta ricevuto o inviato dall'utente viene intercettato dal componente.
2. L'e-mail viene suddivisa in diverse parti: l'intestazione, il corpo del messaggio e gli allegati.
3. Il corpo e gli allegati del messaggio (inclusi gli oggetti OLE) vengono sottoposti a scansione per escludere la presenza di oggetti pericolosi. Gli oggetti dannosi vengono rilevati utilizzando i database dell'applicazione e l'algoritmo euristico. Il database contiene le descrizioni di tutti i programmi dannosi attualmente conosciuti, nonché i metodi che consentono di neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti nel database.
4. Dopo la scansione anti-virus, è possibile eseguire le azioni seguenti:

   - Se il corpo o gli allegati del messaggio contengono codice dannoso, Anti-Virus Posta blocca l'e-mail, inserisce una copia dell'oggetto infetto nel *backup* ed effettua un tentativo di disinfezione dell'oggetto. Se l'e-mail viene disinfettata correttamente, diventa nuovamente disponibile. Se la disinfezione non riesce, l'oggetto infetto nell'e-mail viene eliminato. Dopo la scansione anti-virus, nella riga dell'oggetto del messaggio compare un testo che segnala che è in corso l'elaborazione del messaggio da parte dell'applicazione.

- Se nel corpo o in un allegato viene rilevato codice potenzialmente dannoso, la cui pericolosità non è tuttavia garantita, la parte sospetta del messaggio viene spostata in un'area di archiviazione speciale denominata *Quarantena*.
- Se all'interno del messaggio non viene individuato alcun codice dannoso, il messaggio viene reso immediatamente disponibile all'utente.

Per Microsoft Office Outlook viene fornito un modulo di estensione integrato (vedere la sezione "Scansione della posta elettronica in Microsoft Office Outlook" a pag. 61) che consente l'ottimizzazione della scansione della posta elettronica.

Se si utilizza il client di posta The Bat!, è possibile utilizzare la applicazione insieme con altre applicazioni anti-virus. Le regole per l'elaborazione del traffico di posta elettronica (vedere la sezione "Scansione della posta elettronica nel plugin di The Bat!" a pag. 62) vengono configurate direttamente in The Bat! e sovrascrivono le impostazioni di protezione della posta elettronica dell'applicazione.

Se si lavora con altri programmi di posta (inclusi Microsoft Outlook Express/Windows Mail, Mozilla Thunderbird, Eudora e Incredimail), Anti-Virus Posta esamina i messaggi sui protocolli SMTP, POP3, IMAP, e NNTP.

VEDERE ANCHE

Anti-Virus Posta..56

MODIFICA DEL LIVELLO DI PROTEZIONE

Il livello di protezione è definito come configurazione preimpostata delle impostazioni di Anti-Virus Posta. Gli specialisti di Kaspersky Lab distinguono tre livelli di protezione. Per decidere quale livello selezionare, l'utente deve considerare le condizioni operative e la situazione corrente.

- Se si lavora in un ambiente non protetto, è consigliabile impostare il livello di protezione alto. Un esempio di ambiente di questo tipo è rappresentato da una connessione a un servizio di posta elettronica gratuito, da una rete priva di protezione centralizzata della posta elettronica.
- Il livello consigliato garantisce un equilibrio ottimale tra efficienza e protezione ed è adatto nella maggior parte dei casi. Rappresenta anche l'impostazione predefinita.
- Se si lavora in un ambiente ben protetto, è possibile utilizzare il livello di protezione basso. Un esempio di ambiente di questo tipo è rappresentato da una rete aziendale con protezione centralizzata della posta elettronica.

Se nessuno dei livelli preimpostati soddisfa le proprie esigenze, è possibile modificare manualmente le impostazioni di Anti-Virus Posta (vedere la sezione "Anti-Virus Posta" a pag. 56). Di conseguenza, il nome del livello di protezione cambierà in **Personalizzato**. Per ripristinare le impostazioni predefinite del componente, selezionare uno dei livelli di protezione preimpostati.

➡ *Per modificare il livello di protezione della posta elettronica preimpostato:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Posta**.
4. Selezionare il livello di protezione desiderato nella finestra visualizzata.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

Anti-Virus Posta esamina un messaggio di posta elettronica. Se la scansione indica che il messaggio o una delle sue parti (corpo, allegato) è infetto o potenzialmente infetto, le successive operazioni del componente dipendono dallo stato dell'oggetto e dall'azione selezionata.

Come risultato della scansione, Anti-Virus Posta assegna uno degli stati seguenti agli oggetti rilevati:

- stato programma dannoso (ad esempio *virus*, *Trojan*);
- *potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che il messaggio di posta o l'allegato contiene una sequenza di codice di un virus sconosciuto o un codice modificato di un virus conosciuto.

Per impostazione predefinita, quando viene rilevato un oggetto pericoloso o potenzialmente infetto Anti-Virus Posta visualizza un messaggio di avviso e propone una scelta di azioni da eseguire per l'oggetto.

Tutte le azioni possibili sono mostrate nella tabella seguente.

SE L'AZIONE SCELTA È	SE VIENE RILEVATO UN OGGETTO PERICOLOSO
Richiedi intervento utente	Anti-Virus Posta visualizzerà un messaggio di avviso contenente informazioni sul programma dannoso che ha infettato, o potenzialmente infettato, il file, offrendo la possibilità di scegliere una delle azioni indicate di seguito.
Blocca l'accesso	Anti-Virus Posta blocca l'accesso all'oggetto. Le informazioni rilevanti vengono registrate nel rapporto. In un secondo momento sarà possibile provare a disinfettare l'oggetto.
Blocca l'accesso ☑ **Disinfetta**	Anti-Virus Posta blocca l'accesso all'oggetto e tenta di disinfettarlo. Se la disinfezione riesce, viene ripristinato al suo uso normale. Se non è possibile disinfettare l'oggetto, viene messo in quarantena. Le informazioni rilevanti vengono registrate nel rapporto. In un secondo momento sarà possibile provare a disinfettare l'oggetto.
Blocca l'accesso ☑ **Disinfetta** ☑ **Elimina se la disinfezione non riesce**	Anti-Virus Posta blocca l'accesso all'oggetto e tenta di disinfettarlo. Se la disinfezione riesce, viene ripristinato al suo uso normale. Se la disinfezione non riesce, l'oggetto viene eliminato. Una copia dell'oggetto viene archiviata nel Backup. Gli oggetti etichettati come *potenzialmente infetti* vengono messi in quarantena.
Blocca l'accesso ☐ **Disinfetta** ☑ **Elimina**	Quando Anti-Virus Posta rileva un oggetto infetto o potenzialmente infetto, il componente lo elimina senza informare l'utente.

Prima di eseguire la disinfezione o l'eliminazione di un oggetto, Anti-Virus Posta ne crea una copia di backup, archiviandola in backup. In questo modo, l'oggetto può essere ripristinato o disinfettato in futuro.

➡ *Per modificare l'azione da eseguire sugli oggetti rilevati, eseguire le operazioni seguenti:*

1. Aprire la finestra principaledell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Posta**.
4. Selezionare l'azione desiderata nella finestra che viene visualizzata.

CREAZIONE DI UN AMBITO DI PROTEZIONE

Per ambito di protezione si intende il tipo di messaggi da esaminare. Per impostazione predefinita, Kaspersky Anti-Virus esamina sia i messaggi in entrata che in uscita. Se si imposta la scansione solo per i messaggi in entrata, si consiglia di analizzare i messaggi in uscita all'avvio dell'applicazione, poiché il computer potrebbe contenere worm di posta elettronica che utilizzano i messaggi come canale di proliferazione. Questa misura precauzionale contribuirà a evitare situazioni spiacevoli spesso causate da invii non controllati di grandi quantità di messaggi di posta infetti provenienti dal proprio computer.

L'ambito di protezione include inoltre

- le impostazioni utilizzate per l'integrazione di Anti-Virus Posta nel sistema e i protocolli da esaminare. Per impostazione predefinita, il componente Anti-Virus Posta è integrato nei client di posta Microsoft Office Outlook e The Bat!.
- i protocolli esaminati. Anti-Virus Posta esegue la scansione dei messaggi di posta elettronica trasmessi tramite i protocolli POP3, SMTP, IMAP e NNTP. Inoltre, il componente esegue la scansione del traffico dei client di messaggistica istantanea ICQ e MSN.

Per disabilitare la scansione della posta in uscita, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Posta**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Generale**, nella sezione **Ambito della protezione** specificare i valori necessari per le impostazioni.

Per specificare le impostazioni di integrazione e i protocolli esaminati, eseguire le operazioni seguenti:

1. Aprire la finestra principaledell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Posta**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Generale**, nella sezione **Integrazione**,selezionare le caselle necessarie.

SELEZIONE DEL METODO DI SCANSIONE

I metodi di scansione consentono la verifica dei collegamenti all'interno dei messaggi di posta elettronica per rilevare se sono inclusi nell'elenco di indirizzi Web sospetti e/o nell'elenco di indirizzi di phishing.

Il controllo che tali collegamenti non siano inclusi nell'elenco di indirizzi di phishing consente di evitare attacchi di phishing, che si presentano sotto forma di messaggi di posta elettronica provenienti da sedicenti istituti finanziari contenenti collegamenti ai relativi siti Web. Il testo del messaggio induce il lettore a cliccare sul collegamento e a immettere informazioni riservate nella finestra che segue, ad esempio, un numero di carta di credito o il nome utente e la password usati per collegarsi al proprio sito di Internet banking per eseguire operazioni finanziarie.

Un attacco di phishing può essere mascherato, ad esempio, da lettera proveniente dalla propria banca con un collegamento al relativo sito Web ufficiale. Facendo clic sul collegamento, si arriva a una copia identica del sito della banca che visualizza addirittura l'indirizzo effettivo nel browser, anche se in realtà di tratta di un sito falso. Da questo

momento in poi, tutte le operazioni eseguite nel sito possono essere ricostruite e utilizzate per prelevare denaro dal conto dell'utente.

Il controllo dei collegamenti per verificare che non siano inclusi nell'elenco di indirizzi Web sospetti consente di tenere traccia dei siti Web inclusi nell'elenco Bloccati. L'elenco viene creato dagli specialisti di Kaspersky Lab ed è integrato nel pacchetto di installazione dell'applicazione.

Per eseguire la scansione dei collegamenti nei messaggi utilizzando il database di indirizzi sospetti, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Posta**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Generale**, sezione **Metodi di scansione**, selezionare la casella **Confronta gli URL con il database degli indirizzi sospetti**.

Per eseguire la scansione dei collegamenti nei messaggi utilizzando il database di indirizzi di phishing, eseguire le operazioni seguenti:

1. Aprire la finestra principaledell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Posta**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Generale**, sezione **Metodi di scansione**, selezionare la casella **Confronta gli URL con il database degli indirizzi di phishing**.

SCANSIONE DELLA POSTA ELETTRONICA IN MICROSOFT OFFICE OUTLOOK

Se si utilizza Microsoft Office Outlook come client di posta, è possibile definire configurazioni personalizzate per le scansioni anti-virus.

Durante l'installazione dell'applicazione, in Microsoft Office Outlook viene integrato un plugin speciale. che consente di configurare velocemente le impostazioni del componente Anti-Virus Posta e di determinare i messaggi di posta elettronica che verranno esaminati per cercare eventuali oggetti pericolosi.

Il plugin si presenta sotto forma di una scheda speciale denominata **Anti-Virus Posta** che si trova nel menu **Strumenti** → **Opzioni**. Questa scheda consente di specificare le modalità di scansione della posta.

Per specificare condizioni di filtraggio complesse:

1. Aprire la finestra principaledell'applicazione Microsoft Outlook.
2. Selezionare **Strumenti** → **Opzioni** dal menu dell'applicazione.
3. Selezionare la scheda **Anti-Virus Posta**, specificare la modalità di scansione della posta necessaria.

SCANSIONE DELLA POSTA ELETTRONICA NEL PLUG-IN THE BAT!

Le azioni da intraprendere sugli oggetti di posta infetti nel client The Bat! vengono definite mediante gli strumenti del programma stesso.

Le impostazioni di Anti-Virus Posta che definiscono l'esecuzione della scansione dei messaggi in entrata e in uscita, nonché le azioni sugli oggetti di posta elettronica pericolosi e le esclusioni, vengono ignorate se la scansione dei messaggi ricevuti tramite i protocolli POP3, SMTP, IMAP, MAPI e NNTP risulta disabilitata. L'unica azione presa in considerazione da The Bat! è la scansione degli archivi allegati.

Le impostazioni di protezione della posta elettronica si estendono a tutti i moduli anti-virus installati nel computer che supportano The Bat!

È importante ricordare che i messaggi di posta elettronica in entrata vengono esaminati prima dal componente Anti-Virus Posta e solo successivamente dal plugin del client di posta di The Bat!. Se viene rilevato un oggetto dannoso, Kaspersky Anti-Virus informerà immediatamente l'utente. Se si seleziona l'azione **Disinfetta** (**Elimina**) nella finestra di notifica di Anti-Virus Posta, le azioni mirate all'eliminazione della minaccia verranno eseguite da questo componente. Se si seleziona l'azione **Salta** nella finestra di notifica, l'oggetto verrà disinfettato dal plug-in The Bat!. Quando si inviano messaggi di posta elettronica, la scansione viene eseguita prima dal plug-in, quindi da Anti-Virus Posta.

È necessario decidere:

- quale flusso di messaggi di posta elettronica sarà esaminato (in arrivo, in uscita);
- in quale momento gli oggetti della posta elettronica saranno analizzati (all'apertura di un messaggio o prima del salvataggio su disco);
- le azioni eseguite dal client di posta quando vengono rilevati oggetti pericolosi nei messaggi di posta elettronica. È ad esempio possibile selezionare:
  - **Tenta di disinfettare le parti infette –** effettua un tentativo di disinfezione dell'oggetto di posta infetto, che rimane nel messaggio se l'operazione non riesce.
  - **Elimina parti infette –**elimina l'oggetto pericoloso nel messaggio, indipendentemente dal fatto che sia infetto o sospetto.

Per impostazione predefinita, The Bat! trasferisce tutti gli oggetti di posta infetti nella cartella Quarantena senza tentare di disinfettarli.

The Bat! non inserisce intestazioni speciali nei messaggi contenenti oggetti pericolosi nel caso in cui la scansione della posta elettronica ricevuta tramite i protocolli POP3, SMTP, IMAP, MAPI e NNTP sia disabilitata. Se la scansione è abilitata, nei messaggi verranno inserite intestazioni speciali.

➡ *Per impostare le regole di protezione della posta in The Bat!:*

1. Aprire la finestra principale di The Bat!.
2. Selezionare **Impostazioni** dal menu **Proprietà** del client di posta.
3. Selezionare **Protezione anti-virus** nella struttura ad albero delle impostazioni.

UTILIZZO DELL'ANALISI EURISTICA

Il metodo euristico implica l'analisi delle attività eseguite dall'oggetto nel sistema. Se tali azioni sono tipiche di oggetti dannosi, è probabile che l'oggetto venga classificato come dannoso o sospetto. In questo modo è possibile rilevare le

nuove minacce prima ancora che queste vengano studiate dagli analisti anti-virus. L'analisi euristica è abilitata per impostazione predefinita.

Inoltre, è possibile impostare il livello di dettaglio delle scansioni, **Superficiale**, **Medio** o **Approfondito**. A tale scopo, sposta il cursore nella posizione selezionata.

Per abilitare/disabilitare l'analisi euristica e impostare il livello di dettaglio della scansione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Posta**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nelle finestra visualizzata, all'interno della scheda **Prestazioni**, nella sezione **Metodi di scansione**, selezionare / deselezionare la casella **Analisi euristica** e impostare il livello di dettaglio della scansione.

SCANSIONE DEI FILE COMPOSITI

La selezione della modalità di scansione dei file composti influisce sulle prestazioni di Kaspersky Anti-Virus. È possibile abilitare o disabilitare la scansione degli oggetti allegati e limitare le dimensioni massime degli archivi da esaminare.

Per configurare le impostazioni di scansione dei file compositi:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Posta**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Prestazioni**, selezionare la modalità di scansione dei file composti.

FILTRO DEGLI ALLEGATI

È possibile configurare il filtro delle condizioni degli oggetti allegati al messaggio di posta elettronica. L'uso del filtro consente di migliorare la protezione del computer, in quanto nella maggior parte dei casi i programmi dannosi si diffondono attraverso l'invio di allegati. Rinominando o eliminando determinati tipi di allegato, è possibile proteggere il computer da potenziali pericoli, ad esempio l'apertura automatica degli allegati alla ricezione di un messaggio.

Se il computer non è protetto da alcun software di rete locale e se si accede a Internet direttamente senza un server proxy o un firewall, si consiglia di non disabilitare la scansione degli archivi allegati.

Per configurare le impostazioni di filtraggio degli allegati:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Posta**.
4. Nel menu a discesa, fare clic sul pulsante **Personalizza**.

5. Nella finestra visualizzata, all'interno della scheda **Filtro allegati**, specificare le condizioni di filtro degli allegati di posta elettronica. Selezionando una delle ultime due modalità, l'elenco di tipi di file diventa attivo e consente di specificare i tipi necessari o di aggiungere una maschera per la selezione di un nuovo tipo.

   Se è necessario aggiungere una maschera di un nuovo tipo, fare clic sul collegamento **Aggiungi** e immettere i dati richiesti nella finestra **Maschera nome file** che viene visualizzata.

RIPRISTINO DELLE IMPOSTAZIONI DI PROTEZIONE DELLA POSTA ELETTRONICA PREDEFINITE

Quando si configura Anti-Virus Posta, è sempre possibile ripristinarne le impostazioni consigliate. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Esse sono raggruppate nel livello di protezione **Consigliato**.

➡ *Per ripristinare le impostazioni predefinite relative alla posta, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Posta**.
4. Nella finestra visualizzata, fare clic sul pulsante **Livello predefinito**.

STATISTICHE DELLA PROTEZIONE DELLA POSTA ELETTRONICA

Tutte le operazioni eseguite dal componente Anti-Virus Posta vengono registrate in un rapporto speciale che riepiloga i dettagli delle operazioni eseguite dal componente, raggruppate nelle schede seguenti:

- Tutti gli oggetti pericolosi rilevati nei messaggi di posta elettronica da Anti-Virus Posta vengono elencati nella scheda *Rilevati*. Per ogni oggetto viene indicato il nome completo e lo stato assegnato dall'applicazione durante la scansione o l'elaborazione. Se il componente ha individuato con successo il programma che ha infettato l'oggetto, a quest'utlimo verrà assegnato lo stato appropriato: ad esempio *virus*, *Trojan* e così via. Se non è possibile stabilire con esattezza il tipo di effetto dannoso, all'oggetto verrà assegnato lo stato *sospetto*. Accanto allo stato viene visualizzata anche l'azione applicata all'oggetto (rilevato, non trovato, disinfettato).

  Per non visualizzare nella scheda le informazioni sugli oggetti di posta elettronica disinfettati, deselezionare la casella ☑ **Mostra oggetti disinfettati**.

- L'elenco completo degli eventi verificatisi durante l'uso di Anti-Virus Posta è riportato nella scheda *Eventi*. Gli eventi possono avere i seguenti stati:

  - *informativo* (ad esempio oggetti non elaborati, ignorati in base al tipo);
  - *avviso* (ad esempio se viene rilevato un virus);
  - *commento* (ad esempio se un archivio è protetto da password).

  Solitamente, i messaggi informativi sono esclusivamente di riferimento e non rivestono particolare interesse. È possibile disabilitare la visualizzazione dei messaggi informativi. Per effettuare questa operazione, deselezionare la casella ☑ **Mostra tutti gli eventi**.

- Le *statistiche* di scansione vengono visualizzate nella scheda relativa. In questa scheda sarà riportato il numero totale di oggetti di posta elettronica analizzati, quindi, suddivisi in colonne, verranno indicati: il numero di archivi

presenti sul numero totale di oggetti analizzati, il numero di oggetti pericolosi, il numero di oggetti disinfettati, il numero di oggetti in quarantena e così via.

- Le impostazioni applicate da Anti-Virus Posta vengono visualizzate nella scheda *Impostazioni*. Utilizzare il collegamento **Modifica impostazioni** per configurare rapidamente il componente.

➡ *Per visualizzare informazioni sulle attività del componente, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Rapporto** dal menu di scelta rapida del componente **Anti-Virus Posta**.

ANTI-VIRUS WEB

Ogni volta che si naviga in Internet, si espongono le informazioni memorizzate nel computer al rischio di essere infettate da programmi pericolosi che possono accedere al computer mentre si visualizza una pagina Web.

Kaspersky Anti-Virus 6.0 per Windows Workstations MP4 comprende un componente speciale chiamato *Anti-Virus Web* per garantire la protezione delle sessioni Internet. Esso protegge il computer dai dati che arrivano attraverso il protocollo HTTP e inoltre previene l'esecuzione di script pericolosi sul computer.

La protezione Web monitora esclusivamente il traffico HTTP che attraversa le porte indicate nell'elenco delle porte monitorate (vedere la sezione "Creazione di un elenco delle porte monitorate" a pagina 172). Nel pacchetto di installazione di Kaspersky Anti-Virus è incluso un elenco delle porte comunemente utilizzate per il trasferimento della posta elettronica e del traffico HTTP. Se si usano porte non comprese nell'elenco, è consigliabile aggiungerle per proteggere il traffico che le attraversa.

Se si lavora in una zona non protetta, navigando in Internet per mezzo di un modem, è consigliabile utilizzare Firewall per usufruire di una protezione. Se il computer è inserito in una rete protetta da un firewall o da filtri del traffico HTTP, Firewall fornisce un'ulteriore protezione durante l'uso di Internet.

Una serie di impostazioni, suddivisa in cosiddetti livelli di protezione, determina la modalità di scansione del traffico. Se Anti-Virus Web rileva una minaccia, eseguirà l'azione assegnata.

Il livello di protezione del traffico Web è determinato da un insieme di impostazioni. Tali impostazioni possono essere suddivise nei gruppi seguenti:

- impostazioni dell'ambito di protezione;
- impostazioni che determinano l'efficienza della protezione del traffico (utilizzo dell'analisi euristica, ottimizzazione della scansione).

Kaspersky Lab consiglia di evitare di configurare manualmente le impostazioni di Anti-Virus Web. Nella maggior parte dei casi è sufficiente selezionare un livello di protezione diverso.

Se Anti-Virus Web è stato disabilitato per qualche motivo, le connessioni stabilite prima che sia stato abilitato non verranno monitorate. È necessario riavviare il browser immediatamente dopo l'avvio di Anti-Virus Web.

➡ *Per modificare le impostazioni di Anti-Virus Web:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Web**.
4. Nella finestra visualizzata, apportare le modifiche desiderate alle impostazioni del componente.

IN QUESTA SEZIONE

Algoritmo di funzionamento del componente 67

Modifica del livello di protezione del traffico HTTP 68

Modifica delle azioni da eseguire sugli oggetti rilevati 68

Creazione di un ambito di protezione 69

Selezione del metodo di scansione 69

Utilizzo dell'analisi euristica 70

Ottimizzazione della scansione 70

Ripristino delle impostazioni di protezione Web predefinite 71

Statistiche di Anti-Virus Web 71

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Anti-Virus Web protegge le informazioni ricevute attraverso il traffico HTTP e impedisce l'esecuzione sul computer di script pericolosi.

In questa sezione viene descritto in modo più dettagliato il funzionamento del componente. Il traffico HTTP viene protetto mediante l'algoritmo seguente:

1. Anti-Virus Web intercetta e analizza per escludere la presenza di codice dannoso ogni pagina Web o file cui l'utente o una determinata applicazione può accedere attraverso il protocollo HTTP. Gli oggetti dannosi vengono rilevati utilizzando i database dell'applicazione e l'algoritmo euristico. Il database contiene le descrizioni di tutti i programmi dannosi attualmente conosciuti, nonché i metodi che consentono di neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti nel database.

2. Dopo l'analisi è possibile agire come segue:

   - Se una pagina Web o un oggetto al quale l'utente cerca di accedere contengono codice dannoso, ne verrà bloccato l'accesso. Viene visualizzata una notifica relativa all'infezione dell'oggetto o della pagina richiesta.

   - Se il file o la pagina Web non contiene codice dannoso, l'utente potrà accedervi direttamente.

Gli script vengono esaminati secondo l'algoritmo seguente:

1. Ogni esecuzione di uno script su una pagina Web viene intercettata da Anti-Virus Web e analizzata per individuare eventuali codici dannosi.

2. Se lo script contiene codice dannoso, Anti-Virus Web lo blocca, informando l'utente con un apposito messaggio a comparsa.

3. Se nello script non viene rilevato alcun codice dannoso, esso viene eseguito.

L'applicazione è dotata di un plug-in speciale per Microsoft Internet Explorer che si integra nel browser durante la procedura di installazione. La presenza del plug-in è indicata dalla comparsa di un nuovo pulsante nella barra degli strumenti del browser. Facendo clic su di esso viene aperta una scheda informativa riportante le statistiche di Anti-Virus Web sul numero di script esaminati e bloccati.

VEDERE ANCHE

Anti-Virus Web 66

MODIFICA DEL LIVELLO DI PROTEZIONE DEL TRAFFICO HTTP

Il livello di protezione è definito come configurazione preimpostata delle impostazioni di Anti-Virus Web. Gli specialisti di Kaspersky Lab distinguono tre livelli di protezione. Per decidere quale livello selezionare, l'utente deve considerare le condizioni di funzionamento e la situazione in cui viene utilizzata l'applicazione:

- Il livello di protezione Alto è consigliato in ambienti sensibili in cui non vengono utilizzati altri strumenti di protezione HTTP.
- Il livello di protezione Consigliato rappresenta la scelta ideale nella maggior parte delle situazioni.
- Il livello di protezione Basso viene consigliato se nel computer sono installati altri strumenti di protezione del traffico HTTP.

Se nessuno dei livelli preimpostati soddisfa le proprie esigenze, è possibile configurare le impostazioni di Anti-Virus Web in modo individuale. Di conseguenza, il nome del livello di protezione cambierà in **Personalizzato**. Per ripristinare le impostazioni predefinite del componente, selezionare uno dei livelli di protezione preimpostati.

➡ *Per modificare il livello di protezione preimpostato per il traffico Web:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Web**.
4. Selezionare il livello di protezione desiderato nella finestra visualizzata.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

Se l'analisi di un oggetto HTTP indica che questo contiene codice dannoso, la risposta del componente Anti-Virus Web dipende dall'azione selezionata dall'utente.

Anti-Virus Web blocca sempre le azioni eseguite da oggetti pericolosi e visualizza dei messaggi a comparsa che comunicano all'utente l'azione intrapresa.

Vengono riportati di seguito i dettagli delle possibili opzioni di elaborazione degli oggetti HTTP pericolosi.

SE L'AZIONE SCELTA È	SE VIENE RILEVATO UN OGGETTO PERICOLOSO NEL TRAFFICO HTTP
Richiedi intervento utente	Anti-Virus Web visualizza un messaggio di avviso contenente informazioni sul codice dannoso che potrebbe aver infettato l'oggetto e consente di scegliere come procedere.
Blocca	Anti-Virus Web blocca l'accesso all'oggetto e informa l'utente mediante la visualizzazione di un messaggio. Le stesse informazioni saranno registrate nel rapporto.

Permetti	Anti-Virus Web consente l'accesso all'oggetto. Le informazioni rilevanti vengono registrate nel rapporto.

Per modificare l'azione da eseguire sugli oggetti rilevati, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Web**.
4. Selezionare l'azione desiderata nella finestra che viene visualizzata.

CREAZIONE DI UN AMBITO DI PROTEZIONE

L'ambito di protezione rappresenta un elenco di indirizzi attendibili che non verranno sottoposti a una scansione anti-virus da parte del componente di protezione. Creare un elenco del genere può risultare utile, ad esempio, nei casi in cui Anti-virus Web interferisce con il download di un file specifico.

Per creare l'elenco di indirizzi attendibili:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Web**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra **Impostazioni personalizzate: Anti-Virus Web** visualizzata, sezione **URL attendibili**, fare clic sul pulsante **Aggiungi**.
6. Nella finestra **Maschera indirizzo (URL)** visualizzata, immettere un indirizzo attendibile (o la relativa maschera).

SELEZIONE DEL METODO DI SCANSIONE

I metodi di scansione consistono nella verifica dei collegamenti per controllare che non siano inclusi nell'elenco di indirizzi sospetti e/o nell'elenco di indirizzi di phishing.

Il controllo dei collegamenti per verificare che non siano inclusi nell'elenco di indirizzi di phishing consente di evitare attacchi di phishing, che si presentano sotto forma di messaggi di posta elettronica provenienti da sedicenti istituti finanziari e contengono collegamenti ai relativi siti Web. Il testo del messaggio induce il lettore a cliccare sul collegamento e a immettere informazioni riservate nella finestra che segue, ad esempio, un numero di carta di credito o il nome utente e la password usati per collegarsi al proprio sito di Internet banking per eseguire operazioni finanziarie.

Poiché è possibile ricevere il collegamento a un sito di phishing non solo in un messaggio di posta elettronica (vedere la sezione "Selezione del metodo di scansione" a pagina 60) ma anche in molti altri modi, ad esempio nel testo di un messaggio ICQ, il componente Anti-Virus Web tiene traccia dei tentativi di accesso a un sito di phishing a livello di scansione del traffico HTTP e li blocca.

Il controllo dei collegamenti per verificare che non siano inclusi nell'elenco di indirizzi Web sospetti consente di tenere traccia dei siti Web inclusi nell'elenco Bloccati. L'elenco viene creato dagli specialisti di Kaspersky Lab ed è integrato nel pacchetto di installazione dell'applicazione.

Per eseguire la scansione dei collegamenti nei messaggi utilizzando il database di indirizzi Web sospetti, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Web**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra **Impostazioni personalizzate: Anti-Virus Web** visualizzata, sezione **Metodi di scansione**, selezionare la casella ☑ **Confronta gli URL con il database degli indirizzi sospetti**.

Per eseguire la scansione dei collegamenti utilizzando il database degli indirizzi di phishing, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Web**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra **Impostazioni personalizzate: Anti-Virus Web** visualizzata, sezione **Metodi di scansione**, selezionare la casella ☑ **Confronta gli URL con il database degli indirizzi di phishing**.

UTILIZZO DELL'ANALISI EURISTICA

Il metodo euristico implica l'analisi delle attività eseguite dall'oggetto nel sistema. Se tali azioni sono tipiche di oggetti dannosi, è probabile che l'oggetto venga classificato come dannoso o sospetto. In questo modo è possibile rilevare le nuove minacce prima ancora che queste vengano studiate dagli analisti anti-virus. L'analisi euristica è abilitata per impostazione predefinita.

Kaspersky Anti-Virus notifica il rilevamento di oggetti dannosi con un messaggio. È necessario rispondere alla notifica selezionando un'azione.

Inoltre, è possibile impostare il livello di dettaglio delle scansioni, **Superficiale**, **Medio** o **Approfondito**, spostando il cursore nella posizione selezionata.

Per utilizzare l'analisi euristica e impostare il livello di dettaglio delle scansioni, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Web**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra **Impostazioni personalizzate: Anti-Virus Web** visualizzata, sezione **Metodi di scansione**, selezionare la casella ☑ **Analisi euristica** e specificare il livello di dettaglio della scansione in basso.

OTTIMIZZAZIONE DELLA SCANSIONE

Per rilevare il codice dannoso in modo più efficiente, il componente Anti-Virus Web memorizza nel buffer frammenti di oggetti scaricati da Internet. Quando si utilizza questo metodo, un oggetto viene esaminato solo dopo essere stato scaricato completamente. L'oggetto viene quindi sottoposto all'analisi anti-virus e, a seconda del risultato, l'applicazione restituisce l'oggetto all'utente oppure lo blocca.

La memorizzazione nel buffer comporta tuttavia un aumento dei tempi di elaborazione dell'oggetto e di conseguenza dei tempi di restituzione all'utente. Questo può causare problemi durante la copia e l'elaborazione di oggetti di grandi dimensioni in quanto è possibile che la connessione al client HTTP raggiunga il timeout.

Per risolvere questo problema, si consiglia di ridurre il tempo di memorizzazione nel buffer dei frammenti di oggetti Web scaricati da Internet. Allo scadere di questo limite temporale, l'utente riceve la parte scaricata e non esaminata del file. L'oggetto viene sottoposto a una scansione anti-virus solo dopo essere stato copiato completamente. In questo modo si può ridurre l'attesa nella restituzione degli oggetti e risolvere il problema delle interruzioni nelle connessioni Internet senza abbassare il relativo livello di protezione.

Per impostazione predefinita, il tempo di memorizzazione nel buffer dei frammenti di file è limitato a un secondo. Aumentando questo valore o disattivando il tempo limite di memorizzazione nel buffer si migliorano le scansioni anti-virus, ma si rallenta la restituzione dell'oggetto.

Per limitare il tempo di memorizzazione dei frammenti di file nel buffer:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Web**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza**.
5. Nella finestra **Impostazioni personalizzate: Anti-Virus Web** visualizzata, sezione **Ottimizzazione della scansione**, selezionare la casella **Limita il tempo di caching dei frammenti** e immettere il valore temporale (in secondi) nel campo corrispondente.

RIPRISTINO DELLE IMPOSTAZIONI DI PROTEZIONE WEB PREDEFINITE

Quando si configura Anti-Virus Web, è sempre possibile ripristinarne le impostazioni consigliate. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Esse sono raggruppate nel livello di protezione **Consigliato**.

Per ripristinare le impostazioni predefinite di Anti-Virus Web, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Virus Web**.
4. Nella finestra visualizzata, fare clic sul pulsante **Livello predefinito**.

STATISTICHE DI ANTI-VIRUS WEB

Informazioni di carattere generale sulle attività eseguite da Anti-Virus Web vengono salvate in un rapporto speciale che riepiloga i dettagli delle attività eseguite dal componente, raggruppate in schede:

- Tutti gli oggetti pericolosi rilevati da Anti-Virus Web nel traffico HTTP vengono elencati nella scheda *Rilevati*. che mostra il nome dell'oggetto analizzato e il nome dell'oggetto pericoloso. Per nascondere le informazioni sugli oggetti individuati nel traffico HTTP e disinfettati, deselezionare la casella **Mostra oggetti disinfettati**.
- L'elenco completo degli eventi verificatisi durante l'uso di Anti-Virus Web è riportato nella scheda *Eventi*. Tutti gli eventi sono suddivisi in eventi importanti e notifiche minori. Solitamente, le notifiche minori sono messaggi di riferimento non necessariamente rilevanti. È possibile disattivare la visualizzazione di tali eventi deselezionando la casella **Mostra tutti gli eventi**.
- Le impostazioni applicate da Anti-Virus Web vengono visualizzate nella scheda *Impostazioni*. Utilizzare il collegamento **Modifica impostazioni** per configurare rapidamente il componente.

Per visualizzare informazioni sulle attività del componente, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Rapporto** dal menu di scelta rapida del componente **Anti-Virus Web**.

DIFESA PROATTIVA

Kaspersky Anti-Virus 6.0 per Windows Workstations MP4 protegge sia dalle minacce note sia da quelle sconosciute, sulle quali i database dell'applicazione non contengono alcuna informazione. Questa funzione è garantita dal componente *Difesa Proattiva*.

Le tecnologie preventive offerte da Difesa Proattiva consentono di risparmiare tempo e neutralizzare le nuove minacce prima che possano danneggiare il computer. In che modo? A differenza delle tecnologie reattive, che analizzano il codice in base ai record contenuti nei database dell'applicazione, le tecnologie preventive riconoscono una nuova minaccia tramite una sequenza di azioni eseguite da un programma dannoso. Il programma include una serie di criteri in grado di identificare il livello di pericolosità delle attività di un programma. Se analizzando una sequenza di azioni Kaspersky Anti-Virus ritiene che un programma sia sospetto, l'applicazione esegue l'azione assegnata dalla regola per quel tipo di attività.

Le attività pericolose vengono classificate in base all'insieme totale di azioni del programma. Vengono classificate come attività pericolose:

- le modifiche al file system;
- i moduli che vengono incorporati in altri processi;
- il mascheramento di processi nel sistema;
- la modifica di certe chiavi del registro di sistema di Microsoft Windows.

La Difesa Proattiva viene attuata strettamente in base a impostazioni che definiscono:

- *Se sul computer in uso l'attività dell'applicazione viene monitorata*. Questa modalità di Difesa Proattiva è garantita dal modulo **Analisi Attività Applicazione**. Per impostazione predefinita, questa modalità è abilitata, garantendo un attento monitoraggio delle azioni di qualsiasi programma aperto sul computer.
- *Se le variazioni al registro di sistema vengono monitorate*. Questa modalità di Difesa Proattiva è garantita dal modulo **Controllo del Registro**. Per impostazione predefinita, tale modulo è disabilitato, il che significa che Kaspersky Anti-Virus non analizza i tentativi di apportare modifiche alle chiavi del registro di sistema di Microsoft Windows.

Per modificare le impostazioni di Difesa Proattiva, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Difesa Proattiva**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, apportare le modifiche desiderate alle impostazioni del componente.

IN QUESTA SEZIONE

Algoritmo di funzionamento del componente........74

Analisi Attività Applicazione........74

Registry Guard........79

Statistiche di Difesa Proattiva........82

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Le tecnologie preventive fornite dal componente Difesa Proattiva di Kaspersky Anti-Virus riconoscono una nuova minaccia nel computer in base alle sequenze di azioni eseguite da un determinato programma. Il pacchetto di installazione di Kaspersky Anti-Virus include una serie di criteri in grado di identificare il livello di pericolosità delle attività di un'applicazione. Se analizzando una sequenza di azioni Kaspersky Anti-Virus ritiene che un'applicazione sia sospetta, viene eseguita l'azione specificata dalla regola per il monitoraggio delle attività pericolose.

Di seguito viene illustrato in modo dettagliato l'algoritmo di Difesa Proattiva.

1. Immediatamente dopo l'avvio del computer, Difesa Proattiva analizza i seguenti fattori:

   - *Azioni di ogni applicazione che viene eseguita sul computer*. Difesa Proattiva registra la cronologia delle azioni eseguite in sequenza e la confronta con le sequenze tipiche delle attività pericolose (nel pacchetto di installazione dell'applicazione è incluso un database dei tipi di attività pericolose che viene aggiornato insieme agli altri database dell'applicazione).

   - *Ogni tentativo di modificare il registro di sistema* eliminando o aggiungendo chiavi, assegnando loro valori non appropriati che influenzano le modalità di visualizzazione e modifica, ecc.

2. L'analisi si basa sulle regole Consenti e Blocca di Difesa Proattiva.

3. Dopo l'analisi è possibile agire come segue:

   - Se l'attività soddisfa le condizioni stabilite dalla regola Consenti di Difesa Proattiva o non corrisponde a nessuna regola Blocca, essa non viene bloccata.

   - Se tale attività è descritta da una regola Blocca, il componente agirà in base alle istruzioni specificate nella regola, solitamente bloccando l'esecuzione dell'attività. Sul video verrà visualizzata una notifica che specifica l'applicazione, il suo tipo di attività e la cronologia delle azioni eseguite. L'utente deve decidere se bloccare o consentire questa attività. È inoltre possibile creare una regola per questo tipo di attività e annullare le azioni eseguite sul sistema.

VEDERE ANCHE

Difesa Proattiva 73

ANALISI ATTIVITÀ APPLICAZIONE

Il componente **Analisi Attività Applicazione** di Kaspersky Anti-Virus controlla le attività eseguite sul computer da tutte le applicazioni. L'applicazione include una serie di descrizioni di eventi che possono essere considerati pericolosi. Per ogni evento di questo tipo viene creata una regola di monitoraggio. Se l'attività di un'applicazione è classificata come evento pericoloso, Difesa Proattiva rispetterà in modo rigoroso le istruzioni specificate per la regola relativa a tale evento.

VEDERE ANCHE

Utilizzo dell'elenco di attività pericolose 75

Modifica delle regole per il monitoraggio delle attività pericolose 75

Controllo degli account di sistema 76

Eventi di Difesa Proattiva 76

UTILIZZO DELL'ELENCO DI ATTIVITÀ PERICOLOSE

Tenere presente che la configurazione del controllo delle applicazioni in Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista e Microsoft Windows Vista x64 presenta alcune differenze rispetto alla configurazione di un'applicazione installata su altri sistemi operativi.

Specifiche per la configurazione del controllo delle attività delle applicazioni in Microsoft Windows XP

Kaspersky Anti-Virus controlla l'attività delle applicazioni sul computer. Difesa Proattiva reagisce immediatamente a una sequenza definita di azioni delle applicazioni. Le sequenze pericolose di azioni includono:

- azioni tipiche di programmi Trojan;
- tentativi di intercettazione della tastiera;
- installazione nascosta di driver;
- tentativi di modifica del kernel del sistema operativo;
- tentativi di creazione di oggetti e processi nascosti con PID negativo;
- tentativi di modifica dei file HOSTS;
- tentativi di implementazione in altri processi;
- rootkit che reindirizzano l'input/output dei dati;
- tentativi di invio di richieste DNS.

L'elenco di attività pericolose viene aggiunto automaticamente in seguito all'aggiornamento di Kaspersky Anti-Virus e non è modificabile. È tuttavia possibile disabilitare il monitoraggio di un'attività pericolosa.

➡ *Per disattivare il monitoraggio di un'attività pericolosa:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Difesa Proattiva**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Analisi Attività Applicazione**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra **Impostazioni: Analisi Attività Applicazione** visualizzata, deselezionare la casella ☑ accanto al nome dell'attività che non si desidera monitorare.

Specifiche per la configurazione del controllo delle attività delle applicazioni in Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64 o Microsoft Windows 7 x64

Se il computer è in esecuzione in uno dei sistemi operativi indicati sopra, il controllo non verrà applicato a ogni evento a causa delle caratteristiche specifiche di tali sistemi.

MODIFICA DELLE REGOLE PER IL MONITORAGGIO DELLE ATTIVITÀ PERICOLOSE

L'elenco di attività pericolose viene aggiunto automaticamente in seguito all'aggiornamento di Kaspersky Anti-Virus e non è modificabile. È possibile:

- disattivare il monitoraggio di un'attività pericolosa (vedere pagina 75);

- modificare la regola utilizzata da Difesa Proattiva quando viene rilevata un'attività pericolosa;
- creare un elenco di esclusioni (vedere pagina 151), elencando le applicazioni la cui attività non viene considerata pericolosa.

Per modificare la regola:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Difesa Proattiva**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Analisi Attività Applicazione**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra **Impostazioni: Analisi Attività Applicazione** visualizzata, sezione **Eventi**, selezionare l'evento per il quale si desidera modificare la regola.
6. Configurare la regola per l'evento selezionato utilizzando i collegamenti nella sezione di descrizione:
   - fare clic sul collegamento con l'azione preimpostata e selezionare l'azione desiderata nella finestra **Seleziona azione** visualizzata;
   - fare clic sul collegamento con il periodo di tempo preimpostato (non per tutti i tipi di attività) e specificare l'intervallo di scansione per i processi nascosti nella finestra **Rilevamento processi nascosti** visualizzata;
   - fare clic sul collegamento **Attivato / Disattivato** per indicare se si desidera creare il rapporto sull'esecuzione dell'attività.

CONTROLLO DEGLI ACCOUNT DI SISTEMA

Gli account utente controllano l'accesso al sistema e identificano l'utente e il relativo ambiente di lavoro, impedendo ad altri utenti di danneggiare il sistema operativo e i dati. I processi di sistema sono processi avviati dagli account utente di sistema.

Se si desidera controllare l'attività dei processi di sistema oltre a quella dei processi utente mediante Kaspersky Anti-Virus, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Difesa Proattiva**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Analisi Attività Applicazione**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra **Impostazioni: Analisi Attività Applicazione** visualizzata, sezione **Generale**, selezionare la casella ☑ **Effettua il monitoraggio degli account utente del sistema**.

EVENTI DI DIFESA PROATTIVA

Questa sezione fornisce informazioni sugli eventi di Difesa Proattiva che possono essere considerati pericolosi. Tenere presente che ogni evento non deve essere interpretato inequivocabilmente come una minaccia. Alcune di queste operazioni fanno parte del comportamento comune delle applicazioni in esecuzione sul computer oppure possono essere considerate come una reazione del sistema operativo alle caratteristiche funzionali delle applicazioni. Tuttavia, in alcuni casi tali eventi possono risultare causati dall'attività di un intruso o da un programma dannoso. Pertanto, è importante sapere che l'attivazione di Difesa Proattiva non indica necessariamente che l'attività rilevata è stata causata da un programma dannoso: essa può essere anche dovuta ad un programma comune innocuo che presenta alcune caratteristiche tipiche di un programma dannoso.

Attività tipiche di worm P2P / Attività tipiche di Trojan

Un worm è un programma auto-replicante che si diffonde attraverso le reti di computer. I worm P2P si diffondono in modalità di connessione "computer-computer", bypassando la gestione centralizzata. Di regola, tali worm si diffondono attraverso cartelle di rete condivise e supporti rimovibili.

Un Trojan è un programma dannoso che penetra nel computer travestito da programma innocuo. Gli hacker caricano i Trojan su risorse di rete aperte, supporti di dati disponibili per la registrazione su computer e su supporti rimovibili, quindi li distribuiscono utilizzando servizi di messaggistica (come la posta elettronica) in modo che vengano eseguiti sui computer.

Tra le attività tipiche di tali programmi:

- azioni tipiche di un oggetto dannoso che penetra e si insedia nel sistema;
- azioni dannose vere e proprie;
- azioni tipiche di un oggetto dannoso che si diffonde.

Keylogger

Un keylogger è un programma che intercetta ogni pressione di tasti sulla tastiera. Tale programma dannoso può inviare qualunque informazione digitata alla tastiera (codici di accesso, password, numeri di carta di credito) ad un intruso. Tuttavia, la funzione di intercettazione dei tasti premuti può essere utilizzata anche da comuni programmi legittimi. Un esempio di tali programmi è un videogioco che deve intercettare i dati digitati alla tastiera dall'utente durante il funzionamento a schermo intero. Inoltre, l'intercettazione dei tasti premuti viene utilizzata spesso per attivare una funzione di un programma da un altro programma mediante i cosiddetti "tasti di scelta rapida".

Installazione nascosta di driver

L'installazione nascosta di driver è il processo di installazione di un driver di un programma dannoso compiuta per ottenere un accesso di basso livello al sistema operativo nascondendo il programma dannoso persistente nel sistema e rendendo complicata la sua rimozione. Il processo di installazione nascosta può essere rilevato utilizzando strumenti comuni (come Task Manager di Microsoft Windows). Poiché durante l'installazione del driver non appare alcuna finestra di installazione standard, è difficile per l'utente sospettare di dover tenere traccia dei processi in esecuzione nel sistema.

Tuttavia, in alcuni casi Difesa Proattiva può restituire un falso allarme. Ad esempio, i videogiochi più recenti sono protetti dalla copia e distribuzione non autorizzate. Per questo motivo, tali videogiochi installano alcuni driver di sistema sul computer dell'utente. Tali attività possono essere classificate in alcuni casi come "installazione nascosta di driver".

Modifica del kernel del sistema operativo

Il kernel del sistema operativo consente alle applicazioni in esecuzione sul computer un accesso coordinato alle risorse del computer: CPU, RAM e hardware esterno. Alcuni programmi dannosi possono tentare di modificare la logica del kernel del sistema operativo reindirizzando a se stessi le richieste inviate da driver standard. Quando i programmi dannosi ottengono un accesso di basso livello al sistema operativo in questo modo, tentano di nascondere la loro presenza e complicano il processo della loro rimozione dal sistema.

Un esempio di falso allarme restituito da Difesa Proattiva è la reazione del componente a determinati sistemi di crittografia sviluppati per le unità disco rigido. Tali sistemi sono sviluppati per assicurare una protezione completa dei dati e installano un driver nel sistema, insediandosi nel kernel del sistema operativo per poter intercettare le richieste ai file sul disco rigido ed eseguire le operazioni di crittografia/decrittografia.

Oggetti nascosti / Processi nascosti

Un processo nascosto è un processo che non può essere rilevato mediante strumenti comuni (come Task Manager di Microsoft Windows, Process Explorer, ecc.). Rootkit (ossia "kit sviluppato per ottenere privilegi root") è un programma o una raccolta di programmi per il controllo nascosto di un sistema violato da un hacker. Questo termine è stato importato dall'ambiente Unix.

In ambiente Microsoft Windows, rootkit indica di solito un programma di mascheramento che si insedia nel sistema, intercetta e falsifica i messaggi di sistema contenenti le informazioni sui processi in esecuzione nel sistema e sul

contenuto delle cartelle sull'unità disco. In altre parole, un rootkit funziona in modo simile ad un server proxy, in quanto consente a determinati dati di transitare inalterati nel tentativo di bloccare o falsificare il resto dei dati. Inoltre, di solito un rootkit può mascherare la presenza di qualunque processo, cartella e file memorizzato su un'unità disco e di chiavi di registro, se queste sono descritte nella sua configurazione. Numerosi programmi di mascheramento installano i propri driver e servizi nel sistema, rendendoli "invisibili" sia a strumenti di gestione del sistema (come Task Manager o Process Explorer) che ad applicazioni anti-virus.

Un caso particolare di processo nascosto è quello di un'attività consistente nel tentativo di creare processi nascosti con valori di PID negativi. Un PID è il numero di identificazione personale che il sistema operativo assegna a ciascun processo in esecuzione. Il PID è univoco per ciascun processo in esecuzione ed è statico per ognuno di essi nella sessione corrente del sistema operativo. Se il PID di un processo ha un valore negativo, questo processo è nascosto e non può essere rilevato mediante strumenti comuni.

Un esempio di falso allarme è l'attivazione di Difesa Proattiva in risposta ad applicazioni di gioco che proteggono i propri processi da strumenti di utilità di hacking sviluppati per evadere le restrizioni sulle licenze o fornire soluzioni e scorciatoie di gioco.

Modifica dei file HOSTS

Il file hosts è uno dei più importanti file di sistema di Microsoft Windows. È stato studiato per reindirizzare l'accesso alle risorse Web convertendo gli indirizzi URL in indirizzi IP non presso i server DNS, ma strettamente su un computer locale. Il file hosts è un file in semplice formato testo in cui ogni riga determina la corrispondenza tra il nome simbolico (URL) di un server e il suo indirizzo IP.

I programmi dannosi utilizzano spesso questo file per riassegnare gli indirizzi dei server di aggiornamento di applicazioni anti-virus al fine di bloccare gli aggiornamenti ed impedire il rilevamento dei programmi dannosi stessi mediante il metodo di firma, e per altri scopi.

Reindirizzamento dell'input-output

Il punto debole essenziale consiste nell'esecuzione di una riga di comando con reindirizzamento dell'input/output (di solito sulla rete), la quale può essere utilizzata di solito per ottenere un accesso remoto al computer.

Un oggetto dannoso tenta di ottenere l'accesso alla riga di comando di un computer bersaglio, che verrà poi sfruttato per eseguire comandi. L'accesso può essere ottenuto di solito dopo un attacco remoto e l'esecuzione di uno script che utilizza questa vulnerabilità. Lo script esegue l'interprete della riga di comando dal computer connesso tramite TCP. A questo punto l'intruso può gestire il sistema in remoto.

Intrusione in un processo / Intrusione in tutti i processi

Esistono molti tipi di programmi dannosi mascherati come file eseguibili, librerie o moduli di estensione di programmi noti, che possono fare intrusione in processi standard. Grazie a questi programmi, un eventuale intruso può causare perdite di dati sul computer dell'utente. Il traffico di rete creato dal codice dannoso non verrà filtrato dai firewall, in quanto viene percepito come traffico creato da un programma cui è stato concesso l'accesso a Internet.

I Trojan fanno di solito intrusione in altri processi. Tuttavia, tali attività sono tipiche anche di determinati programmi innocui, pacchetti di aggiornamento e procedure di installazione guidata. Ad esempio, i programmi di traduzione fanno intrusione in altri processi per intercettare la pressione di tasti di scelta rapida.

Accesso sospetto al registro di sistema

I programmi dannosi modificano il registro di sistema per poter registrare se stessi per l'esecuzione automatica all'avvio del sistema operativo, cambiare la pagina iniziale in Microsoft Internet Explorer ed eseguire molte altre azioni distruttive. Tuttavia, tenere presente che al registro di sistema possono accedere anche programmi comuni. Ad esempio, i programmi comuni possono utilizzare l'opzione di creazione e sfruttamento di chiavi di registro nascoste per nascondere all'utente proprie informazioni riservate (tra cui informazioni sulla licenza).

I programmi dannosi creano chiavi di registro nascoste che non vengono visualizzate dai programmi comuni (tipo regedit). Vengono create chiavi con nomi non validi per impedire all'editor del registro di sistema di visualizzare tali valori, rendendo complicata la diagnostica della presenza di malware all'interno del sistema.

Invio di dati utilizzo dell applicazioni attendibili

Esistono molti tipi di programmi dannosi mascherati come file eseguibili, librerie o moduli di estensione di programmi noti, che possono fare intrusione in processi standard. Grazie a questi programmi, un eventuale intruso può causare

perdite di dati sul computer dell'utente. Il traffico di rete creato dal codice dannoso non verrà filtrato dai firewall, in quanto viene percepito come traffico creato da un programma cui è stato concesso l'accesso a Internet.

Attività pericolosa nel sistema

Questo punto consiste nel rilevamento di comportamento sospetto di un processo separato: ad esempio, una modifica dello stato del sistema operativo che concede l'accesso diretto alla RAM o l'ottenimento di privilegi di debugger. L'attività intercettata non è tipica per la maggior parte dei programmi, ma è al tempo stesso pericolosa. Pertanto, tale attività viene classificata come sospetta.

Invio di richieste DNS

Il server DNS è progettato per rispondere alle richieste DNS tramite il protocollo corrispondente. Se non viene trovato alcun record corrispondente alla richiesta DNS nel database del server DNS locale, la richiesta verrà ritrasmessa fin quando non raggiunge un server su cui sono memorizzate le informazioni richieste. Poiché le richieste DNS sono lasciate transitare senza scansione dalla maggior parte dei sistemi di protezione, il contenuto di un pacchetto DNS potrebbe includere frammenti aggiuntivi contenenti dati personali dell'utente. Un eventuale intruso che controlla un server DNS che elabora queste richieste DNS ha l'opportunità di acquisire queste informazioni.

Tentativo di accesso a un'area di archiviazione protetta

Un processo tenta di ottenere l'accesso a un'area di archiviazione protetta all'interno del sistema operativo contenente dati personali e password dell'utente.

REGISTRY GUARD

Uno degli obiettivi di molti programmi dannosi è quello di modificare il registro del sistema operativo del computer. Questo obiettivo può essere raggiunto attraverso innocui programmi joke o tramite programmi più dannosi che rappresentano una minaccia reale per il computer.

Ad esempio, i programmi dannosi possono copiare le proprie informazioni sulle chiavi di registro che determinano l'apertura automatica delle applicazioni all'avvio. Di conseguenza, i programmi dannosi verranno avviati automaticamente all'avvio del sistema operativo.

Le modifiche agli elementi del registro di sistema vengono monitorate dall'apposito modulo di Difesa Proattiva, **Registry Guard**.

VEDERE ANCHE

Gestione dell'elenco di regole di monitoraggio del registro di sistema 79

Creazione di un gruppo di elementi del registro di sistema da monitorare 80

GESTIONE DELL'ELENCO DI REGOLE DI MONITORAGGIO DEL REGISTRO DI SISTEMA

Kaspersky Lab ha creato un elenco di regole per controllare le operazioni eseguite sugli elementi del registro e lo ha incluso nel pacchetto di installazione dell'applicazione. Le operazioni eseguite sugli elementi del registro sono suddivise in gruppi logici come *Protezione del sistema*, *Protezione di Internet*, ecc. Ognuno di questi gruppi comprende gli elementi del registro di sistema e le regole per la loro gestione. L'elenco viene aggiornato insieme all'intera applicazione.

Ogni gruppo di regole ha una priorità di esecuzione che è possibile aumentare o diminuire. Più in alto si trova il gruppo, maggiore è la priorità assegnatagli. Se lo stesso elemento del registro è presente in più gruppi, la prima regola applicata è quella del gruppo con la priorità più elevata.

Per aumentare o diminuire la priorità di esecuzione di una regola, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Difesa Proattiva**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Registry Guard**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra **Impostazioni: Registry Guard** visualizzata, utilizzare i pulsanti **Sposta su** / **Sposta giù**.

Per smettere di usare un gruppo di regole, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Difesa Proattiva**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Registry Guard**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra **Impostazioni: Registry Guard** visualizzata, deselezionare la casella accanto al nome del gruppo. Così facendo, il gruppo di regole rimane nell'elenco ma non sarà utilizzato. Si sconsiglia di eliminare un gruppo di regole dall'elenco, poiché contiene un elenco degli elementi del registro di sistema utilizzati più frequentemente dai programmi dannosi.

CREAZIONE DI UN GRUPPO DI ELEMENTI DEL REGISTRO DI SISTEMA DA MONITORARE

È possibile creare i propri gruppi di elementi del registro di sistema monitorati.

Per creare un gruppo di controllo degli elementi del registro di sistema:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Difesa Proattiva**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Registry Guard**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra **Impostazioni: Registry Guard** visualizzata, fare clic sul pulsante **Aggiungi**.
6. Nella finestra visualizzata, immettere il nome del nuovo gruppo di monitoraggio per gli elementi del registro di sistema nel campo **Nome gruppo**.

   Creare un elenco di elementi del registro di sistema da includere nel gruppo nella scheda **Chiavi**.

   Nella scheda **Regole**, creare una regola per gli elementi del registro di sistema selezionati.

VEDERE ANCHE

Selezione degli elementi del registro di sistema per creare una regola..81

Creazione di una regola per il monitoraggio degli elementi del registro di sistema 81

SELEZIONE DEGLI ELEMENTI DEL REGISTRO DI SISTEMA PER CREARE UNA REGOLA

Il gruppo di elementi creato deve contenere almeno un elemento del registro di sistema.

Per aggiungere un elemento del registro di sistema all'elenco, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Difesa Proattiva**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Registry Guard**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra **Impostazioni: Registry Guard** visualizzata, fare clic sul pulsante **Aggiungi**.
6. Nella finestra visualizzata, nella scheda **Chiavi**, fare clic sul pulsante **Aggiungi**.
7. Nella finestra **Specificare un elemento del registro** visualizzata, eseguire le operazioni seguenti:
    a. selezionare un elemento del registro di sistema o un gruppo di elementi per cui si desidera creare una regola di monitoraggio;
    b. specificare il valore dell'elemento o la maschera per un gruppo di elementi cui si desidera applicare la regola nel campo **Valore**;
    c. se si desidera applicare la regola anche a tutte le sottochiavi dell'elemento del registro di sistema selezionato, selezionare la casella **Includi sottochiavi**.

CREAZIONE DI UNA REGOLA PER IL MONITORAGGIO DEGLI ELEMENTI DEL REGISTRO DI SISTEMA

Una regola di monitoraggio degli elementi del registro di sistema consiste nel determinare quanto segue:

- l'applicazione cui dovrà essere applicata la regola se viene rilevato un tentativo di accesso al registro di sistema;
- la reazione del programma a un tentativo di eseguire un'operazione sul registro di sistema da parte di un'applicazione.

Per creare una regola per gli elementi del registro di sistema selezionati, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Difesa Proattiva**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Registry Guard**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra **Impostazioni: Registry Guard** visualizzata, fare clic sul pulsante **Aggiungi**.
6. Nella finestra visualizzata, nella scheda **Regole**, fare clic sul pulsante **Nuovo**. La regola generale verrà aggiunta in cima all'elenco di regole.
7. Selezionare una regola dall'elenco e specificare le impostazioni della regola nella parte inferiore della scheda:
    - Specificare l'applicazione.

Per impostazione predefinita, una regola viene creata per tutte le applicazioni. Se si desidera che una regola riguardi un'applicazione specifica, fare clic su **Qualsiasi** e questo valore si modificherà in **Selezionate**. Quindi fare clic sul collegamento **Specificare nome applicazione**. Verrà aperto un menu di scelta rapida. Selezionare il comando **Sfoglia** per aprire la finestra standard di selezione file; in alternativa, scegliere il comando **Applicazioni** per aprire l'elenco delle applicazioni attualmente in esecuzione e selezionare quella desiderata.

- Specificare la reazione di Difesa Proattiva ai tentativi di leggere, modificare o eliminare elementi del registro del sistema da parte dell'applicazione selezionata.

  Come reazione è possibile scegliere tra: **Consenti**, **Richiedi intervento utente** e **Blocca**. Fare clic sul collegamento dell'azione fino a visualizzare quella desiderata.

- Specificare se è necessario generare un rapporto sull'operazione eseguita. Facendo clic sul collegamento **Registra** / **Non registrare**.

È possibile creare diverse regole e ordinarle per priorità per mezzo dei pulsanti **Sposta su** e **Sposta giù**. Più in alto si trova la regola, maggiore è la priorità assegnatale.

STATISTICHE DI DIFESA PROATTIVA

Tutte le operazioni eseguite da Difesa Proattiva vengono registrate in un rapporto speciale che riepiloga i dettagli delle operazioni eseguite dal componente, raggruppate nelle schede seguenti:

- *Rilevati* – tutti gli oggetti classificati come pericolosi vengono riuniti in questa scheda.
- *Eventi* – gli eventi relativi al controllo delle attività delle applicazioni sono elencati in questa scheda.
- *Registro* – questa scheda contiene tutte le operazioni riguardanti il registro di sistema.
- *Impostazioni* – in questa scheda si trovano le impostazioni seguite per l'esecuzione di Difesa Proattiva.

Per visualizzare informazioni sulle attività del componente, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Rapporto** dal menu di scelta rapida del componente **Difesa Proattiva**. È possibile selezionare il tipo di informazioni in ogni scheda del rapporto, visualizzarle in ordine crescente o decrescente per ogni colonna e cercare informazioni all'interno del rapporto. Per eseguire questa operazione, utilizzare le voci del menu di scelta rapida accessibili facendo clic con il pulsante destro del mouse sulle intestazioni delle colonne del rapporto.

ANTI-SPY

Oggigiorno il malware include sempre più programmi che hanno lo scopo di:

- visualizzare contenuti pubblicitari importuni in browser Web, finestre popup e banner in vari programmi;
- tentare di stabilire connessioni via modem non autorizzate.

I keylogger sono programmati specificamente per impadronirsi di informazioni confidenziali; gli autodialer, i programmi joke e gli adware mirano invece a causare perdite di tempo e denaro. *Anti-Spy* è concepito appositamente per offrire una protezione da questi programmi.

Anti-Spy comprende i moduli seguenti:

- *Anti-Banner (vedere pagina 83)* blocca i messaggi pubblicitari che compaiono su banner speciali nelle pagine Web o incorporati nelle interfacce di vari programmi installati nel computer;
- *Anti-Dialer (vedere pagina 86)* impedisce i tentativi di stabilire connessioni via modem non autorizzate.

➡ *Per modificare le impostazioni di Anti-Spy, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Spy**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, apportare le modifiche desiderate alle impostazioni dei moduli del componente.

IN QUESTA SEZIONE

Anti-Banner 83

Anti-Dialer 86

Statistiche di Anti-Spy 86

ANTI-BANNER

Anti-Banner blocca i messaggi pubblicitari che compaiono su banner speciali nelle pagine Web o incorporati nelle interfacce di vari programmi installati nel computer.

I banner pubblicitari non solo non contengono nessuna informazione utile, ma distraggono l'utente dal lavoro e aumentano il traffico sul computer. Anti-Banner blocca i banner pubblicitari più diffusi. Kaspersky Anti-Virus comprende delle maschere sviluppate proprio a tal fine. È possibile disabilitare il blocco dei banner o creare elenchi personalizzati di banner autorizzati e bloccati.

Per integrare il modulo Anti-Banner nel browser **Opera**, aggiungere la riga seguente al file *standard_menu.ini*, sezione **[Image Link Popup Menu]**: Item, "Nuovo banner" = Copy image address & Execute program, "<unità>\Programmi\Kaspersky Lab\Kaspersky Anti-Virus 6.0 per Windows Workstations MP4\opera_banner_deny.vbs", "//nologo %C". Sostituire <unità> con il nome dell'unità di sistema.

VEDERE ANCHE

Creazione dell'elenco di indirizzi di banner consentiti 84

Creazione dell'elenco di indirizzi di banner bloccati 84

Impostazioni avanzate del componente 84

Esportazione / importazione degli elenchi di banner 85

CREAZIONE DELL'ELENCO DI INDIRIZZI DI BANNER CONSENTITI

Se si verifica la necessità di escludere determinati banner dal blocco, si può creare un elenco di banner consentiti durante l'utilizzo dell'applicazione. Tale elenco contiene le maschere dei banner pubblicitari consentiti.

➡ *Per aggiungere una nuova maschera all'elenco dei consentiti, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Spy**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Anti-Banner**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, nella scheda **Elenco dei banner consentiti**, fare clic sul pulsante **Aggiungi**.
6. Immettere la maschera di un banner consentito nella finestra **Maschera per l'indirizzo (URL)** visualizzata. Per sospendere l'uso di una maschera creata, non occorre eliminarla dall'elenco: è sufficiente deselezionare la casella ☑ corrispondente.

CREAZIONE DELL'ELENCO DI INDIRIZZI DI BANNER BLOCCATI

È possibile creare un elenco di indirizzi di banner vietati, che verranno bloccati da Anti-Banner non appena rilevati.

➡ *Per aggiungere una nuova mascheraalla lista nera, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Spy**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Anti-Banner**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, nella scheda **Elenco dei banner bloccati**, fare clic sul pulsante **Aggiungi**.
6. Immettere la maschera di un banner bloccato nella finestra **Maschera per l'indirizzo (URL)** visualizzata. Per sospendere l'uso di una maschera creata, non occorre eliminarla dall'elenco: è sufficiente deselezionare la casella ☑ corrispondente.

IMPOSTAZIONI AVANZATE DEL COMPONENTE

Gli specialisti di Kaspersky Lab hanno compilato un elenco di maschere di banner pubblicitari in base a ricerche specifiche, e l'hanno incluso nel pacchetto di installazione di Kaspersky Anti-Virus. I banner pubblicitari che

corrispondono alle maschere incluse nell'elenco verranno bloccati dall'applicazione, a meno che il blocco dei banner non sia disabilitato.

Durante la creazione degli elenchi di banner consentiti/bloccati, è possibile immettere l'indirizzo IP del banner o il relativo nome di simbolo (URL). Per evitare duplicati, è possibile utilizzare un'opzione avanzata che consente di convertire gli indirizzi IP in nomi di dominio e viceversa.

Per disabilitare l'utilizzo dell'elenco di banner inclusi nel pacchetto di installazione dell'applicazione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Spy**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Anti-Banner**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, nella scheda **Avanzate**, selezionare la casella **Non usare l'elenco di banner comuni**.

Per utilizzare l'opzione di conversione degli indirizzi IP dei banner in nomi di dominio o dei nomi di dominio in indirizzi IP, eseguire le operazioni seguenti:

1. Aprire la finestra principaledell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Spy**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Anti-Banner**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, nella scheda **Avanzate**, selezionare la casella **Risolvi indirizzi IP in nomi di dominio**.

ESPORTAZIONE / IMPORTAZIONE DEGLI ELENCHI DI BANNER

È possibile copiare da un computer a un altro gli elenchi di banner consentiti e bloccati che sono stati creati. Durante l'esportazione dell'elenco, è possibile copiare solo l'elemento selezionato nell'elenco o l'intero elenco. Durante l'importazione, è possibile scegliere di aggiungere nuovi indirizzi all'elenco esistente o sostituire l'elenco esistente con quello importato.

Per copiare gli elenchi di banner consentiti / bloccati creati, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Spy**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Anti-Banner**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, nella scheda **Elenco dei banner consentiti** (o nella scheda **Elenco dei banner bloccati**), fare clic sui pulsanti **Importa** o **Esporta**.

ANTI-DIALER

Anti-Dialer protegge dai tentativi non autorizzati di stabilire connessioni via modem. Una connessione è considerata segreta se è configurata in modo da non informare l'utente della connessione in corso o se non è effettuata dall'utente stesso. Solitamente, le connessioni segrete sono indirizzate verso numeri telefonici commerciali.

Ogni volta che viene rilevato un tentativo di connessione segreto, viene visualizzato sullo schermo un messaggio specifico che chiede all'utente se bloccare o meno la connessione. Se la connessione non è stata avviata dall'utente, è molto probabile che sia stata richiesta da un programma dannoso. Se si desidera consentire che un certo numero venga digitato senza che ne sia richiesta la conferma, è consigliabile aggiungerlo all'elenco dei numeri attendibili.

Per aggiungere un numero all'elenco dei numeri attendibili, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Dal menu di scelta rapida del componente **Anti-Spy**, selezionare la voce **Impostazioni**.
4. Nella finestra visualizzata, sezione **Anti-Dialer**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra **Impostazioni: Numeri attendibili** visualizzata, fare clic sul pulsante **Aggiungi**.
6. Nella finestra **Numero di telefono** visualizzata, specificare un numero attendibile o una maschera.

STATISTICHE DI ANTI-SPY

Una descrizione dettagliata di tutte le operazioni eseguite per la protezione dalle frodi perpetrate via Internet è riportata in un rapporto speciale. Tutti gli eventi vengono raggruppati in schede in base a quale modulo di Anti-Spy li ha registrati:

- La scheda *Banner* mostra i banner pubblicitari rilevati e bloccati durante la sessione corrente dell'applicazione.
- I tentativi di creare una connessione con numeri telefonici a pagamento compiuti da programmi dannosi vengono registrati nella scheda *Connessioni nascoste*.
- Nella scheda *Impostazioni* si trovano le impostazioni seguite per l'esecuzione di Anti-Spy.

Per visualizzare informazioni sulle attività del componente, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Rapporto** dal menu di scelta rapida del componente **Anti-Spy**. È possibile selezionare il tipo di informazioni in ogni scheda del rapporto, visualizzarle in ordine crescente o decrescente per ogni colonna e cercare informazioni all'interno del rapporto. Per eseguire questa operazione, utilizzare le voci del menu di scelta rapida accessibili facendo clic con il pulsante destro del mouse sulle intestazioni delle colonne del rapporto.

PROTEZIONE DAGLI ATTACCHI DI RETE

Kaspersky Anti-Virus contiene un componente speciale, *Anti-Hacker*, che garantisce la protezione del computer sia nelle reti locali che in Internet. Il computer risulta così protetto a livello di rete e delle applicazioni, oltre che mascherato sulla rete per prevenire gli attacchi.

Esistono due tipi di regole, basati sui due livelli di protezione di Anti-Hacker:

- *Regole di filtraggio pacchetti*. Si tratta di regole utilizzate per applicare restrizioni di carattere generale all'attività di rete, a prescindere dalle applicazioni installate. Esempio: se si crea una regola per i pacchetti che blocca le connessioni in ingresso sulla porta 21, nessuna delle applicazioni che utilizzano quella porta (come un server FTP) sarà accessibile dall'esterno.

- *Regole per applicazioni*. Si tratta di regole utilizzate per applicare restrizioni all'attività di rete per applicazioni specifiche. Esempio: se le connessioni sulla porta 80 vengono bloccate per tutte le applicazioni, è possibile creare una regola che consenta le connessioni su tale porta solo per il browser Firefox.

Esistono due tipi di regole per *consentire* o *bloccare* alcune applicazioni e pacchetti di rete. Il pacchetto di installazione di Kaspersky Anti-Virus include una serie di regole che definiscono l'attività di rete per le applicazioni più diffuse e l'utilizzo dei protocolli e delle porte più diffusi. Il pacchetto di installazione di Kaspersky Anti-Virus include inoltre una serie di regole Consenti per applicazioni attendibili la cui attività di rete non è sospetta.

Per semplificare l'uso delle impostazioni e delle regole, Kaspersky Anti-Virus suddivide l'intero spazio di rete in zone di sicurezza, corrispondenti prevalentemente alle sottoreti cui appartiene il computer dell'utente. È possibile assegnare uno stato a ogni zona (*Internet*, *Rete locale*, *Attendibile*) per determinare l'applicazione delle regole e il monitoraggio dell'attività di rete al suo interno.

Una speciale funzione di Anti-Hacker, la modalità Mascheramento, impedisce il rilevamento del computer dall'esterno. In questo modo, gli hacker non sanno più dove rivolgere il proprio attacco. Questa modalità non pregiudica le prestazioni del computer in Internet (a meno che il computer non sia utilizzato come server).

➡ *Per modificare le impostazioni di Anti-Hacker, eseguire le operazioni seguenti*:

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.

4. Nella finestra visualizzata, apportare le modifiche desiderate alle impostazioni del componente.

IN QUESTA SEZIONE

Schema di funzionamento del componente 88

Modifica del livello di protezione di Anti-Hacker 89

Regole per applicazioni e filtraggio pacchetti 90

Regole per zone di sicurezza 96

Modifica della modalità Firewall 98

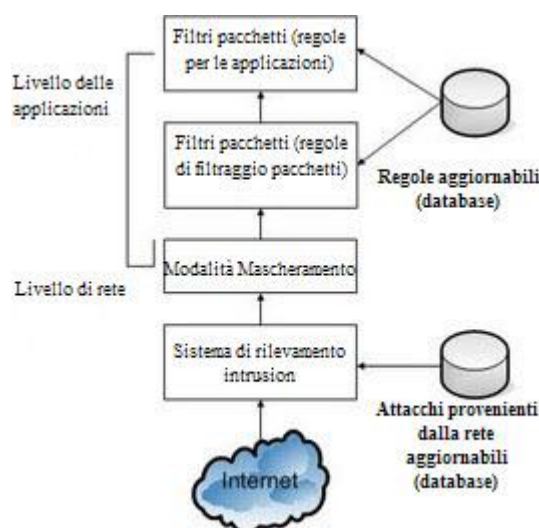
Sistema di rilevamento intrusioni 99

Monitor di rete 100

Tipi di attacchi di rete 100

Statistiche di Anti-Hacker 102

SCHEMA DI FUNZIONAMENTO DEL COMPONENTE

Anti-Hacker protegge il computer a livello di rete e delle applicazioni, mascherandolo inoltre sulla rete per prevenire gli attacchi. Di seguito vengono illustrati in modo dettagliato i principi di funzionamento di Anti-Hacker.

La protezione a livello di rete è garantita da regole globali di filtraggio pacchetti che determinano se le attività di rete sono consentite o bloccate in base all'analisi di vari parametri, quali direzione del trasferimento dei pacchetti, protocollo di trasferimento dei pacchetti di dati e porta pacchetti in uscita. Le regole per i pacchetti stabiliscono l'accesso alla rete, indipendentemente dall'utilizzo della rete da parte delle applicazioni installate nel computer.

Oltre alle regole di filtraggio pacchetti, il *Sistema di rilevamento intrusioni* fornisce ulteriore protezione a livello di rete (vedere la sezione "Sistema di rilevamento intrusioni" a pagina 99). L'obiettivo di questo sottosistema è quello di analizzare le connessioni in ingresso, rilevare le scansioni delle porte del computer e filtrare i pacchetti di rete volti a sfruttare le vulnerabilità del software. Quando è attivato, il Sistema di rilevamento intrusioni blocca per un po' di tempo tutte le connessioni in ingresso provenienti dal computer che intende perpetrare l'attacco. Inoltre viene visualizzato un messaggio che informa l'utente che il computer ha subito un attacco di rete.

L'analisi effettuata dal Sistema di rilevamento intrusioni si basa su uno speciale database degli attacchi di rete (vedere la sezione "Tipi di attacchi di rete" a pagina 100) che viene ampliato regolarmente dagli specialisti di Kaspersky Lab. Il database viene aggiornato insieme agli altri database dell'applicazione.

A livello di applicazioni il computer è protetto dalle regole per l'utilizzo delle risorse di rete definite per le applicazioni installate nel computer. Come per la protezione a livello di rete, la protezione a livello delle applicazioni si basa sull'analisi dei pacchetti di dati in termini di direzione, protocollo di trasferimento e porte utilizzate. Tuttavia, a livello delle applicazioni sono prese in considerazione sia le caratteristiche dei pacchetti di dati sia la specifica applicazione che invia e riceve un certo pacchetto.

L'uso delle regole delle applicazioni consente di configurare la protezione in modo più specifico: ad esempio, un determinato tipo di connessione può essere precluso ad alcune applicazioni ma non ad altre.

VEDERE ANCHE

Protezione dagli attacchi di rete 87

MODIFICA DEL LIVELLO DI PROTEZIONE DI ANTI-HACKER

Quando si utilizza la rete, Kaspersky Anti-Virus protegge il computer a uno dei livelli seguenti:

- **Protezione alta** – livello di protezione in cui le attività della rete sono consentite solo se basate su una regola di autorizzazione. Il comportamento di Anti-Hacker si basa sulle regole incluse nel pacchetto di installazione dell'applicazione o su quelle create dall'utente. La serie di regole fornita con Kaspersky Anti-Virus include le regole Consenti per applicazioni la cui attività di rete non è sospetta e per i pacchetti di dati che possono essere inviati e ricevuti senza alcun rischio. Se tuttavia nell'elenco di regole per un'applicazione esiste una regola Blocca con priorità maggiore rispetto alla regola Consenti, Kaspersky Anti-Virus bloccherà ogni attività di rete per quell'applicazione.

  Se si seleziona questo livello di protezione, tutte le attività di rete non registrate tra le regole Consenti di Anti-Hacker saranno bloccate. Pertanto si raccomanda di utilizzare questo livello solo se si è certi che tutti i programmi necessari sono consentiti dalle regole e se non si prevede di installare nuovo software.

  Tenere presente che a questo livello potrebbe essere pregiudicato il funzionamento di Microsoft Office Outlook. Se il client di posta che elabora i messaggi in ingresso applica delle regole proprie, a questo livello di protezione dagli attacchi di rete i messaggi di posta elettronica non saranno recapitati perché il client di posta non otterrà l'accesso al server di Exchange. Lo stesso effetto potrebbe prodursi se la casella di posta dell'utente è stata trasferita su un nuovo server di Exchange. Per risolvere tali inconvenienti, creare (o modificare se già esistente) una regola Consenti per Microsoft Office Outlook che permetta tutte le attività all'indirizzo IP del server di Exchange.

- **Modalità Apprendimento** – si tratta del livello di protezione al quale vengono create le regole di Anti-Hacker. A questo livello, ogni volta che un programma tenta di utilizzare una risorsa di rete, Anti-Hacker controlla se esiste una regola per tale connessione. In presenza di una regola, Anti-Hacker ne segue le istruzioni. Se non è stata creata nessuna regola, viene visualizzata una descrizione della connessione di rete (quale programma l'ha avviata, su quale porta, con quale protocollo, ecc.). Viene quindi chiesto di decidere se autorizzare la connessione o meno. Facendo clic sull'apposito pulsante nella finestra di notifica, è possibile creare una regola per quella connessione in modo tale che in futuro a quella connessione Anti-Hacker applichi le condizioni della regola senza visualizzare il messaggio.

- **Protezione bassa** – vengono bloccate soltanto le attività di rete esplicitamente vietate. Anti-Hacker blocca l'attività in base alle regole Blocca incluse nel pacchetto di installazione dell'applicazione o a quelle create dall'utente. Se tuttavia nell'elenco di regole per un'applicazione esiste una regola Consenti con priorità maggiore rispetto alla regola Blocca, Kaspersky Anti-Virus consentirà ogni attività di rete per quell'applicazione.

- **Consenti tutto** – si tratta di un livello di protezione che ammette ogni attività di rete nel computer. Si consiglia di impostare questo livello di protezione in pochi casi eccezionali, dove non sono stati osservati attacchi di rete e dove tutta l'attività di rete è considerata attendibile.

È possibile alzare o abbassare il livello di protezione della rete selezionando il livello desiderato oppure modificando le impostazioni per il livello corrente.

Per modificare il livello di protezione contro gli attacchi di rete, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.
4. Nella finestra visualizzata, selezionare il livello di protezione contro gli attacchi di rete desiderato.

REGOLE PER APPLICAZIONI E FILTRAGGIO PACCHETTI

Una regola Firewall è un'azione eseguita da Firewall dopo aver rilevato un tentativo di connessione con determinate impostazioni. È possibile creare:

- Regole per i pacchetti. Le regole per i pacchetti vengono utilizzate per applicare restrizioni ai flussi e ai pacchetti di dati indipendentemente dalle applicazioni.
- Regole per applicazioni. Le regole per applicazioni vengono utilizzate per applicare restrizioni all'attività di rete di una determinata applicazione. Tali regole consentono di ottimizzare il filtraggio, ad esempio quando un determinato tipo di flusso di dati è bloccato per alcune applicazioni ma consentito per altre.

VEDERE ANCHE

Regole per applicazioni: creazione manuale di una regola 90

Regole per applicazioni: creazione di una regola da un modello 91

Regole di filtraggio pacchetti: creazione di una regola 92

Modifica della priorità di una regola 92

Esportazione e importazione delle regole create 93

Ottimizzazione delle regole per applicazioni e filtraggio pacchetti 93

REGOLE PER LE APPLICAZIONI. CREAZIONE MANUALE DI UNA REGOLA

Il pacchetto di installazione di Kaspersky Anti-Virus include una serie di regole per le applicazioni più diffuse nell'ambiente Microsoft Windows. È possibile creare diverse regole Consenti o Blocca per la stessa applicazione. In genere si tratta di applicazioni la cui attività di rete è stata analizzata attentamente da Kaspersky Lab e classificata come pericolosa o sicura in base a criteri rigorosi.

In base al livello di protezione selezionato per Firewall e al tipo di rete nel quale è inserito il computer, l'elenco di regole può essere utilizzato in vari modi. Ad esempio, con il livello **Protezione alta** ogni attività di rete eseguita da applicazioni non contemplate nelle regole Consenti viene bloccata.

Per creare manualmente una regola per applicazioni, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.

4. Nella finestra visualizzata, sezione **Firewall**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, nella scheda **Regole per applicazioni**, fare clic sul pulsante **Aggiungi**. Verrà aperto un menu di scelta rapida. Selezionare il comando **Sfoglia** per aprire la finestra standard di selezione file; in alternativa, scegliere il comando **Applicazioni** per aprire l'elenco delle applicazioni attualmente in esecuzione e selezionare quella desiderata. Verrà visualizzato un elenco di regole per l'applicazione selezionata. Se esistono già delle regole per l'applicazione, saranno elencate tutte nella parte superiore della finestra. Se non esiste nessuna regola, la finestra sarà vuota.

6. Fare clic sul pulsante **Aggiungi** nella finestra delle regole per l'applicazione selezionata.

7. La finestra **Nuova regola** visualizzata contiene un modulo di creazione regole che può essere utilizzato per ottimizzare una regola.

REGOLE PER LE APPLICAZIONI. CREAZIONE DI REGOLE CON MODELLI

Kaspersky Anti-Virus include modelli di regole preimpostati che possono essere utilizzati per creare regole personalizzate.

Le varie applicazioni di rete esistenti possono essere suddivise in alcuni tipi: client di posta, browser Web, ecc. Ciascun tipo è caratterizzato da una serie di attività specifiche, quali l'invio e la ricezione di posta elettronica o il download e la visualizzazione di pagine HTML. Ciascun tipo utilizza un determinato insieme di protocolli e porte di rete. È per questo motivo che disporre di modelli di regole facilita e velocizza la configurazione iniziale delle regole in base al tipo di applicazione.

➡ *Per creare una regola per applicazioni basandosi su un modello, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.

4. Nella finestra visualizzata, sezione **Firewall**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, nella scheda **Regole per applicazioni**, selezionare la casella ☑ **Raggruppa regole per applicazione** (se non è già selezionata), e fare clic sul pulsante **Aggiungi**. Verrà aperto un menu di scelta rapida. Selezionare il comando **Sfoglia** per aprire la finestra standard di selezione file; in alternativa, scegliere il comando **Applicazioni** per aprire l'elenco delle applicazioni attualmente in esecuzione e selezionare quella desiderata. Verrà visualizzata una finestra contenente le regole per l'applicazione selezionata. Se esistono già delle regole per l'applicazione, saranno elencate tutte nella parte superiore della finestra. Se non esiste nessuna regola, la finestra sarà vuota.

6. Fare clic sul pulsante **Modello** nella finestra delle regole per l'applicazione e selezionare un modello di regola dal menu di scelta rapida.

   Consenti tutto è una regola che ammette qualsiasi attività di rete per un'applicazione. **Blocca tutto** è una regola che vieta qualsiasi attività di rete per un'applicazione. Qualsiasi tentativo di avviare una connessione di rete da parte dell'applicazione per cui è stata creata la regola sarà bloccato senza informare l'utente.

   Gli altri modelli elencati nel menu di scelta rapida creano una serie di regole tipiche per i rispettivi programmi. Ad esempio, il modello **Client di posta** crea una serie di regole che autorizzano l'attività di rete standard per i client di posta, come l'invio dei messaggi.

7. Se necessario, modificare le regole create. È possibile modificare l'azione, la direzione della connessione di rete, l'indirizzo, le porte (locali e remote) e l'intervallo temporale da assegnare alla regola.

   Per applicare la regola a un'applicazione aperta con determinate impostazioni di riga di comando, selezionare la casella ☑ **Riga di comando** e immettere la stringa nel campo a destra.

   La regola (o serie di regole) creata sarà aggiunta in coda all'elenco con la priorità più bassa. È possibile aumentare la priorità della regola.

REGOLE PER I FILTRI PACCHETTI. CREAZIONE DI UNA REGOLA

Il pacchetto di installazione di Kaspersky Anti-Virus include una serie di regole che determinano il filtraggio dei pacchetti di dati in ingresso e in uscita dal computer. Il trasferimento dei pacchetti di dati può essere avviato dall'utente stesso o da un'applicazione installata nel computer. Il pacchetto di installazione di Kaspersky Anti-Virus include regole per il filtraggio pacchetti che possono essere applicate a pacchetti le cui modalità di trasmissione sono state analizzate attentamente da Kaspersky Lab e classificate come pericolose o sicure in base a criteri rigorosi.

In base al livello di protezione selezionato per Firewall e al tipo di rete nel quale è inserito il computer, l'elenco di regole può essere utilizzato in vari modi. Ad esempio, con il livello **Protezione alta** ogni attività di rete non contemplata nelle regole Consenti viene bloccata.

Tenere presente che le regole per le zone di sicurezza hanno una priorità maggiore rispetto a quelle di blocco dei pacchetti. Quindi, ad esempio, se si seleziona lo stato **Rete locale** gli scambi di pacchetti saranno consentiti, così come l'accesso alle cartelle condivise, a prescindere dalle regole Blocca dei pacchetti.

Per creare una nuova regola per i pacchetti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.
4. Nella finestra visualizzata, sezione **Firewall**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, nella scheda **Regole di filtraggio pacchetti**, fare clic sul pulsante **Aggiungi**.
6. La finestra **Nuova regola** visualizzata contiene un modulo di creazione regole che può essere utilizzato per ottimizzare una regola.

MODIFICA DELLA PRIORITÀ DI UNA REGOLA

A ogni regola creata per un'applicazione o un pacchetto viene assegnata una certa priorità. A parità di condizioni (quali le impostazioni della connessione di rete), l'azione applicata all'attività dell'applicazione sarà quella della regola con la priorità maggiore.

La priorità di una regola dipende dalla sua posizione nell'elenco delle regole. La prima regola dell'elenco ha la priorità di esecuzione più elevata. Ogni regola creata manualmente viene aggiunta in testa all'elenco. Le regole create da un modello o da una notifica speciale vengono aggiunte in fondo all'elenco delle regole.

Per modificare la priorità di una regola per un'applicazione, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.
4. Nella finestra visualizzata, sezione **Firewall**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, nella scheda **Regole per applicazioni**, selezionare dall'elenco il nome di un'applicazione e fare clic sul pulsante **Modifica**.
6. Nella finestra Regole create visualizzata, utilizzare i pulsanti **Sposta su** e **Sposta giù** per spostare le regole all'interno dell'elenco, modificandone la priorità.

Per modificare la priorità di una regola, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.

4. Nella finestra visualizzata, sezione **Firewall**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, nella scheda **Regole di filtraggio pacchetti**, selezionare una regola. Utilizzare i pulsanti **Sposta su** e **Sposta giù** per spostare la regola all'interno dell'elenco, modificandone la priorità.

ESPORTAZIONE E IMPORTAZIONE DELLE REGOLE CREATE

Le funzioni di esportazione e importazione consentono di trasferire le regole create su altri computer. velocizzando la configurazione di Anti-Hacker.

➡ *Per copiare le regole create per un'applicazione, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.

4. Nella finestra visualizzata, sezione **Firewall**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, nella scheda **Regole per le applicazioni**, fare clic sui pulsanti **Esporta** o **Importa** per copiare le regole.

➡ *Per copiare le regole create per il filtraggio pacchetti, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.

4. Nella finestra visualizzata, sezione **Firewall**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, nella scheda **Regole per i filtri pacchetti**, fare clic sui pulsanti **Esporta** o **Importa** per copiare le regole.

OTTIMIZZAZIONE DELLE REGOLE PER APPLICAZIONI E FILTRAGGIO PACCHETTI

Quando vengono create o modificate, le regole possono essere ottimizzate seguendo le indicazioni seguenti:

- Specificare un nome per la regola. Per impostazione predefinita, l'applicazione utilizza un nome standard che è possibile sostituire.

- Selezionare le impostazioni di connessione di rete che determinano l'applicazione della regola: indirizzo IP remoto, porta remota, indirizzo IP locale, porta locale e durata della regola.

- Modificare le impostazioni di notifica dell'applicazione di una regola.

- Assegnare valori ai parametri della regola e selezionare le azioni da eseguire. L'azione predefinita per ogni regola creata è *Consenti*. Per modificarla in una regola di tipo Blocca, fare clic sul collegamento **Permetti** nella sezione di descrizione della regola. Questo sarà modificato in **Blocca**.

- Definire la direzione della connessione di rete (vedere la sezione "Modifica della direzione di una connessione di rete" a pagina 94) per la regola. Per impostazione predefinita, una regola si applica sia alle connessioni in ingresso sia a quelle in uscita.

- Definire il protocollo utilizzato dalla connessione di rete. Il protocollo predefinito per la connessione è TCP. Se si sta creando una regola per applicazioni, è possibile selezionare il protocollo TCP o UDP. Se si crea una regola per un pacchetto, è possibile modificare il tipo di protocollo (vedere la sezione "Modifica del protocollo di trasferimento dati" a pagina 94). Quando si seleziona ICMP, potrebbe essere necessario indicare anche il tipo (vedere la sezione "Modifica del tipo di pacchetto ICMP" a pagina 96).

- Se sono già state selezionate, specificare le impostazioni precise per la connessione di rete: indirizzo (vedere la sezione "Definizione dell'indirizzo di una connessione di rete" a pagina 95), porta (vedere la sezione "Definizione della porta di connessione" a pagina 95) e intervallo temporale (vedere la sezione "Definizione dell'intervallo temporale per l'attività di una regola" a pagina 95).

- Assegnare priorità alle regole (vedere la sezione "Modifica della priorità della regola" a pagina 92).

È possibile creare una regola dalla finestra di notifica di rilevamento di attività di rete.

La finestra **Nuova regola** contiene un modulo che può essere utilizzato per creare una regola per applicazioni (vedere pagina 90) o per il filtraggio pacchetti (vedere pagina 92).

VEDERE ANCHE

Modifica del protocollo di trasferimento dati 94

Modifica della direzione di una connessione 94

Definizione dell'indirizzo di una connessione di rete 95

Definizione della porta di connessione 95

Definizione dell'intervallo temporale per l'attività di una regola 95

Determinazione del tipo di socket 96

Modifica del tipo di pacchetto ICMP 96

MODIFICA DEL PROTOCOLLO DI TRASFERIMENTO DATI

Una delle proprietà delle regole per applicazioni e per il filtraggio pacchetti è il protocollo di trasferimento dati della connessione di rete. Per impostazione predefinita, quando viene creata una regola viene utilizzato il protocollo TCP sia per le applicazioni sia per i pacchetti.

Per modificare il protocollo di trasferimento dati, eseguire le operazioni seguenti:

1. Nel finestra **Nuova regola** (per le applicazioni vedere pagina 90, per il filtraggio pacchetti vedere pagina 92), sezione **Descrizione regola**, fare clic sul collegamento che riporta il nome del protocollo.

2. Nella finestra **Protocollo** visualizzata, selezionare il valore richiesto.

MODIFICA DELLA DIREZIONE DI UNA CONNESSIONE

Una delle proprietà delle regole per applicazioni e per filtraggio pacchetti è la direzione della connessione di rete.

Se è importante impostare nella regola la direzione esatta dei pacchetti, selezionare se si tratta di pacchetti in ingresso o in uscita. Se si desidera creare una regola per il flusso di dati, selezionare il tipo di flusso: in ingresso, in uscita o entrambi.

La *direzione del flusso* è un parametro diverso dalla *direzione dei pacchetti* perché quando si crea una regola per un flusso si definisce la direzione con cui viene aperta la connessione. Senza prendere in considerazione la direzione dei pacchetti quando si trasferiscono i dati su questa connessione.

Ad esempio, se si configura una regola per lo scambio di dati con un server FTP in esecuzione in modalità passiva, è consigliabile abilitare il flusso in uscita. Per scambiare dati con un server FTP in modalità FTP attiva, è consigliabile abilitare sia i flussi in ingresso sia quelli in uscita.

Per modificare la direzione del flusso di dati, eseguire le operazioni seguenti:

1. Nel finestra **Nuova regola** (per le applicazioni vedere pagina 90, per il filtraggio pacchetti vedere pagina 92), sezione **Descrizione regola**, fare clic sul collegamento che riporta la direzione della connessione.
2. Nella finestra **Seleziona direzione** visualizzata, selezionare il valore desiderato.

DEFINIZIONE DELL'INDIRIZZO DI UNA CONNESSIONE DI RETE

Se per impostare una regola è stato selezionato l'indirizzo IP remoto o locale di una connessione di rete, è consigliabile assegnarle il valore che determinerà l'applicazione della regola.

Per specificare l'indirizzo di una connessione di rete, eseguire le operazioni seguenti:

1. Nella finestra **Nuova regola** (per le applicazioni vedere pagina 90, per il filtraggio pacchetti vedere pagina 92), sezione **Proprietà**, fare clic sulla casella **Indirizzo IP remoto** (o **Indirizzo IP locale**). Quindi, fare clic sul collegamento **Immettere indirizzo IP** nella sezione **Descrizione regola**.
2. Nella finestra **Indirizzo IP** visualizzata, selezionare il tipo di indirizzo IP e immetterne il valore.

DEFINIZIONE DELLA PORTA DI CONNESSIONE

Quando si configurano le regole, è possibile assegnare dei valori alle porte remote o locali.

- Una *porta remota* è la porta di un computer remoto con cui si desidera stabilire una connessione.
- Una *porta locale* è una porta del computer dell'utente.

Le porte locali e remote per il trasferimento di dati vengono definite correttamente quando una regola viene creata direttamente da una notifica di attività sospetta. In questo caso tali informazioni vengono registrate automaticamente.

Per specificare la porta mentre si configurano le regole, eseguire le operazioni seguenti:

1. Nel finestra **Nuova regola** (per le applicazioni vedere pagina 90, per il filtraggio pacchetti vedere pagina 92), sezione **Proprietà**, selezionare la casella **Porta remota** (o **Porta locale**). Quindi, fare clic sul collegamento **Inserire porta** nella sezione **Descrizione regola**.
2. Nella finestra **Porta** visualizzata, immettere un valore per una porta o un intervallo di porte.

DEFINIZIONE DELL'INTERVALLO TEMPORALE PER L'ATTIVITÀ DI UNA REGOLA

È possibile assegnare a ogni regola un intervallo temporale di applicabilità nel corso della giornata. Ad esempio, è possibile bloccare ICQ dalle ore 9:30 alle 6:30.

Per impostare l'orario di applicazione della regola, eseguire le operazioni seguenti:

1. Nel finestra **Nuova regola** (per le applicazioni vedere pagina 90, per il filtraggio pacchetti vedere pagina 92), sezione **Proprietà**, selezionare la casella **Intervallo di tempo**. Quindi, fare clic sul collegamento **Specificare l'intervallo di tempo** nella sezione **Descrizione regola**.

2. Nella finestra **Intervallo di tempo** visualizzata, impostare l'intervallo temporale per la regola per mezzo dei campi **da** e **a**.

DETERMINAZIONE DEL TIPO DI SOCKET

È possibile definire per ogni regola il tipo di socket che supporta il trasferimento di dati tramite uno o più protocolli specificati.

Per modificare il tipo di socket, eseguire le operazioni seguenti:

1. Nella finestra **Nuova regola** (per le applicazioni, vedere pagina 90), sezione **Proprietà**, selezionare la casella **Tipo di socket**. Quindi, fare clic sul collegamento che riporta il nome del tipo di socket installato nella sezione **Descrizione regola**.

2. Nella finestra **Tipo di socket** visualizzata, selezionare il valore desiderato per l'impostazione.

MODIFICA DEL TIPO DI PACCHETTO ICMP

Il protocollo ICMP (Internet Control Message Protocol) è stato sviluppato per informare il mittente di un pacchetto di eventuali errori o complicazioni sorti durante il trasferimento dei dati.

Se si seleziona ICMP come protocollo di trasferimento dati di una regola di filtraggio pacchetti che viene creata, è possibile specificare anche il tipo di messaggio ICMP.

Ad esempio, sfruttando l'utilità Ping e facendole inviare determinate interrogazioni ICMP, un hacker potrebbe interpretare le risposte ricevute e scoprire se il computer è acceso o meno. Il pacchetto di installazione dell'applicazione include una regola che blocca le interrogazioni ICMP e le relative risposte, impedendo in questo modo attacchi potenziali al computer.

Per modificare il tipo di pacchetto ICMP, eseguire le operazioni seguenti:

1. Nel finestra **Nuova regola** (per i pacchetti, vedere pagina 92), sezione **Proprietà**, selezionare la casella **Tipo ICMP**. Quindi, fare clic sul collegamento che riporta il nome del tipo di pacchetto ICMP installato nella sezione **Descrizione regola**.

2. Nella finestra **Tipo di pacchetto ICMP** visualizzata, selezionare il valore desiderato.

REGOLE PER ZONE DI SICUREZZA

Dopo l'installazione, Anti-Hacker analizza l'ambiente di rete del computer. In base ai risultati dell'analisi, l'intero spazio di rete viene suddiviso in zone standard:

- *Internet* – il World Wide Web. In questa zona, Kaspersky Anti-Virus opera come firewall personale. Regole predefinite per i pacchetti e le applicazioni disciplinano tutta l'attività di rete per garantire una protezione massima. Quando si lavora in questa zona, le impostazioni di protezione non possono essere modificate, se non per attivare la modalità Mascheramento per una protezione maggiore.

- *Zone di sicurezza* – si tratta di determinate zone standard corrispondenti per lo più alle sottoreti in cui è incluso il computer (sottoreti locali domestiche o al lavoro). Per impostazione predefinita, le attività svolte in queste zone sono definite a medio rischio. È possibile modificare lo stato di queste zone in base a quanto si ritiene affidabile una determinata sottorete, e configurare regole per il filtraggio pacchetti e le applicazioni.

Se è abilitata la modalità Apprendimento di Anti-Hacker, ogni volta che il computer si connette a una nuova zona verrà visualizzata una finestra che ne riporta una breve descrizione. È consigliabile assegnare uno stato alla zona, poiché l'attività di rete sarà autorizzata o meno in base a tale impostazione:

- **Internet**. Questo è lo stato predefinito assegnato a Internet, poiché in questa zona il computer è potenzialmente esposto a tutti i tipi di minacce. Si consiglia di selezionare questo stato per le reti non protette da applicazioni

anti-virus, firewall, filtri e così via. Quando si seleziona tale stato, l'applicazione garantisce la protezione massima per la zona in questione:

- blocco di qualsiasi attività di rete NetBIOS all'interno della sottorete;
- regole Blocca per applicazioni e filtraggio pacchetti che consentono un'attività NetBIOS all'interno della sottorete.

Anche se è stata creata una cartella condivisa, le informazioni nella stessa non saranno disponibili per utenti appartenenti a sottoreti con questo stato. Inoltre, se questo stato è selezionato per una certa sottorete, non sarà possibile accedere ai file e alle stampanti di altri computer di tale sottorete.

- **Rete locale**. L'applicazione assegna questo stato alla maggior parte delle zone di sicurezza rilevate durante l'analisi dell'ambiente di rete del computer, fatta eccezione per le zone Internet. Questo stato è consigliabile per le aree con un fattore di rischio medio, ad esempio le reti LAN aziendali. Se si seleziona questo stato, l'applicazione consente:
  - qualsiasi attività di rete NetBIOS all'interno della sottorete;
  - l'uso di regole per applicazioni e filtraggio pacchetti che consentono un'attività NetBIOS all'interno della sottorete.

  Selezionare questo stato per consentire l'accesso a certe cartelle o stampanti sul computer ma bloccare qualsiasi altra attività esterna.

- **Attendibili**. Si consiglia di applicare questo stato alle aree che si ritiene siano assolutamente sicure e in cui il computer non è soggetto ad attacchi e tentativi di accesso ai dati. Se si seleziona questo stato, tutte le attività di rete saranno consentite. Anche se si seleziona il livello **Protezione alta** e vengono create le regole Blocca, queste non verranno applicate ai computer remoti appartenenti a una zona attendibile.

Tenere presente che qualsiasi restrizione o accesso ai file ha valore solo all'interno di questa sottorete.

È possibile utilizzare la modalità Mascheramento per godere di una protezione maggiore quando si usano reti contrassegnate come **Internet**. In questa modalità sono infatti consentite soltanto le attività di rete avviate dal computer in uso, cosicché il computer risulta invisibile per l'ambiente circostante. Questa modalità non pregiudica le prestazioni del computer su Internet.

Si sconsiglia l'uso della modalità Mascheramento se il computer viene utilizzato come server (ad esempio come server di posta o HTTP). Altrimenti i computer che si connettono al server non lo potranno visualizzare all'interno della rete.

VEDERE ANCHE

Aggiunta di nuove zone di sicurezza 97

Modifica dello stato di una zona di sicurezza 98

Abilitazione / disabilitazione della modalità Mascheramento 98

AGGIUNTA DI NUOVE ZONE DI SICUREZZA

L'elenco delle zone sulle quali è registrato il computer è visualizzato nella scheda **Zone**. A ogni zona è assegnato uno stato, con una breve descrizione della rete e l'indicazione dell'eventuale uso della modalità Mascheramento.

Per aggiungere una nuova zona all'elenco, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.

4. Nella finestra visualizzata, sezione **Firewall**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, nella scheda **Zone**, fare clic sul pulsante **Aggiorna**. Anti-Hacker cercherà le potenziali zone di registrazione, chiedendo eventualmente di selezionare uno stato da assegnare a quelle rilevate. È possibile inoltre aggiungere nuove zone all'elenco manualmente (ad esempio se si connette il laptop a una nuova rete). Per eseguire questa operazione, fare clic sul pulsante **Aggiungi** e immettere le informazioni necessarie nella finestra **Impostazioni zona** visualizzata.

   Per eliminare la rete dall'elenco, fare clic sul pulsante **Elimina**.

MODIFICA DELLO STATO DI UNA ZONA DI SICUREZZA

Quando si aggiungono nuove zone automaticamente, l'indirizzo e la subnet mask vengono determinati automaticamente dall'applicazione. Il programma assegna a ogni zona aggiunta lo stato predefinito **Rete locale**, che può comunque essere modificato.

➧ *Per modificare lo stato della zona di sicurezza, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.

4. Nella finestra visualizzata, sezione **Firewall**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, nella scheda **Zone**, selezionare una zona dall'elenco e fare clic sul collegamento corrispondente della sezione **Descrizione regola** sotto l'elenco. È possibile eseguire operazioni simili e modificare indirizzi e subnet mask nella finestra **Impostazioni zona**, accessibile facendo clic sul pulsante **Modifica**.

ABILITAZIONE / DISABILITAZIONE DELLA MODALITÀ MASCHERAMENTO

La modalità Mascheramento può essere abilitata anche quando si utilizzano reti contrassegnate come **Internet**.

➧ *Per abilitare la modalità Mascheramento, eseguire le operazioni seguenti:*

1. Aprire la finestra principaledell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Selezionare la voce Impostazioni dal menu di scelta rapida del componente **Anti-Hacker**.

4. Nella finestra visualizzata, sezione **Firewall**, fare clic sul pulsante **Impostazioni**.

5. Nella finestra visualizzata, nella scheda **Zone**, selezionare una zona dall'elenco e fare clic sul collegamento corrispondente della sezione **Descrizione regola** sotto l'elenco.

MODIFICA DELLA MODALITÀ FIREWALL

La modalità Firewall controlla la compatibilità di Anti-Hacker con le applicazioni che stabiliscono più connessioni di rete e con i giochi in rete.

- **Compatibilità massima** – Firewall garantisce che Anti-Hacker operi in modo ottimale con le applicazioni che stabiliscono più connessioni di rete (client di reti di condivisione file). Questa modalità potrebbe produrre un rallentamento nel tempo di reazione delle applicazioni di rete, dato che le regole Consenti hanno una priorità maggiore rispetto alla modalità Mascheramento (quest'ultima, infatti, consente soltanto le attività di rete avviate dal computer in uso). Se si riscontrano problemi del genere, si consiglia di utilizzare la modalità **Velocità massima**.
- **Velocità massima** – Firewall garantisce i migliori tempi di reazione possibili per le applicazioni in rete. Tuttavia, in questa modalità si potrebbero riscontrare problemi di connessione in alcune applicazioni di rete, dato che in modalità Mascheramento tutte le connessioni in ingresso e in uscita vengono bloccate a prescindere dalle regole create. Per risolvere il problema, disabilitare la modalità Mascheramento.

Le modifiche alla modalità Firewall avranno effetto solo in seguito al riavvio di Anti-Hacker.

Per modificare la modalità di funzionamento predefinita di Firewall, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.
4. Nella finestra visualizzata, sezione **Firewall**, fare clic sul pulsante **Impostazioni**.
5. Nella finestra visualizzata, nella scheda **Avanzate**, sezione **Modalità Firewall**, selezionare la modalità desiderata.

SISTEMA DI RILEVAMENTO INTRUSIONI

Tutti gli attacchi di rete attualmente noti che potrebbero mettere in pericolo un computer sono elencati nei database dell'applicazione. Il **Sistema rilevamento intrusioni** di Anti-Hacker si basa un elenco di attacchi di questo tipo. L'elenco degli attacchi rilevabili da questo modulo viene aggiornato durante l'aggiornamento dei database (vedere la sezione "Aggiornamento dell'applicazione" a pagina 135). Per impostazione predefinita, Kaspersky Anti-Virus non aggiorna i database relativi agli attacchi.

Il Sistema di rilevamento intrusioni rileva l'attività di rete tipica degli attacchi di rete, e se individua un tentativo di attacco al computer, blocca tutta l'attività di rete tra tale computer e quello dell'utente per un'ora. Sullo schermo verrà visualizzato un avviso che comunica un tentativo di attacco di rete, con informazioni specifiche sul computer di origine dell'attacco. Il Sistema di rilevamento intrusioni può essere sospeso o disabilitato.

Per disabilitare il Sistema di rilevamento intrusioni, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.
4. Nella finestra visualizzata, deselezionare la casella **Abilita Sistema di rilevamento intrusioni**.

   Per arrestare il modulo senza aprire la finestra delle impostazioni dell'applicazione, selezionare la voce **Termina** dal menu di scelta rapida del componente.

Per bloccare per un po' di tempo il computer da cui proviene l'attacco, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Hacker**.

4. Nella finestra visualizzata, sezione **Sistema di rilevamento intrusioni**, selezionare la casella ☑ **Blocca il computer che attacca per... min.** e immettere l'intervallo di tempo (in minuti) nel campo corrispondente.

MONITOR DI RETE

È possibile visualizzare le informazioni dettagliate su tutte le connessioni stabilite nel computer, le porte aperte e il volume di traffico in ingresso e in uscita. Per eseguire questa operazione, utilizzare il comando **Monitor rete** del menu di scelta rapida.

Nella finestra visualizzata le informazioni sono raggruppate nelle schede seguenti:

- *Connessioni stabilite* – questa scheda riporta tutte le connessioni di rete attualmente attive sul computer in uso. L'elenco comprende sia le connessioni avviate dal computer dell'utente sia quelle in ingresso.
- *Porte aperte* – questa scheda elenca tutte le porte aperte sul computer.
- *Traffico* – questa scheda visualizza il volume di informazioni scambiate (in ricezione e in invio) tra il computer in uso e gli altri computer della rete in cui si sta lavorando.

TIPI DI ATTACCHI DI RETE

Esistono attualmente numerosi attacchi di rete che sfruttano le vulnerabilità dei sistemi operativi e di altro software, di sistema o applicazioni, installato nel computer. I pirati informatici sviluppano continuamente nuovi metodi di attacco, imparando come trafugare informazioni confidenziali, provocare anomalie di funzionamento del sistema o assumere il pieno controllo del computer per utilizzarlo come componente di una rete fantasma per sferrare nuovi attacchi.

Per garantire la protezione del computer, è consigliabile conoscere i tipi di attacchi possibili. Gli attacchi di rete noti possono essere suddivisi in tre categorie principali:

- **Scansione porte** – non si tratta di un attacco vero e proprio, bensì di una minaccia che in genere precede un attacco, in quanto rappresenta uno dei modi più comuni per ottenere informazioni su un computer remoto. Le porte UDP / TCP utilizzate dagli strumenti di rete sul computer preso di mira vengono esaminate al fine di rilevarne lo stato (aperta o chiusa).

  Attraverso la scansione delle porte, un hacker è in grado di individuare i tipi di attacchi più efficaci e quelli più deboli. Le informazioni ottenute (un modello del sistema) gli consentono anche di conoscere il sistema operativo utilizzato nel computer remoto. Circoscrivendo ulteriormente in questo modo il numero degli attacchi possibili e, di conseguenza, il tempo necessario per realizzarli. L'ulteriore vantaggio per l'hacker è la possibilità di tentare di utilizzare le vulnerabilità specifiche di quel sistema operativo.

- **Attacchi DoS (Denial of Service)** – si tratta di attacchi che provocano l'instabilità o il blocco di un sistema. Questi attacchi possono danneggiare o corrompere le risorse informative prese di mira, lasciandole inutilizzabili.

  Esistono due tipi principali di attacchi DoS:

  - invio al computer bersaglio di pacchetti appositamente creati e inattesi, che determinano il riavvio o l'arresto del sistema;
  - invio al computer bersaglio di molti pacchetti in rapidissima successione, per renderne impossibile l'elaborazione, in modo da esaurire le risorse di sistema.

  Quelli descritti di seguito sono esempi comuni di attacchi di questo tipo:

  - *Ping of death*: consiste nell'invio di un pacchetto ICMP di dimensioni maggiori di quella massima di 64 KB. Questo attacco può causare il blocco di alcuni sistemi operativi.
  - *Land*: consiste nell'invio a una porta aperta nel computer bersaglio di una richiesta di stabilire una connessione con se stessa. Questo manda il computer in un ciclo che intensifica il carico sul processore e può terminare con il blocco di alcuni sistemi operativi.

- *ICMP Flood*: consiste nell'invio al computer di un elevato numero di pacchetti ICMP. Il computer tenta di rispondere a ogni pacchetto in arrivo, rallentando notevolmente il processore.
- *SYN Flood*: consiste nell'invio di un elevato numero di interrogazioni al computer remoto per stabilire una finta connessione. Il sistema riserva determinate risorse a ciascuna di queste connessioni, esaurendole quindi del tutto e il computer non reagisce più ad altri tentativi di connessione.

- **Attacchi intrusivi**: finalizzati a controllare completamente il computer. Questo è il tipo di attacco più pericoloso poiché, in caso di riuscita, può determinare il controllo completo del computer da parte dell'hacker.

  Gli hacker utilizzano questo tipo di attacco per ottenere informazioni riservate da un computer remoto, ad esempio numeri di carte di credito o password, o per penetrare nel sistema al fine di utilizzarne in seguito le risorse per fini illeciti. Ad esempio, il sistema invaso viene utilizzato come componente di reti fantasma o come piattaforma per nuovi attacchi.

  Questo gruppo è il più grande in termini di numero di attacchi inclusi. Gli attacchi possono essere suddivisi in tre gruppi, a seconda del sistema operativo: attacchi a Microsoft Windows, attacchi a Unix e il gruppo comune per i servizi di rete disponibili in entrambi i sistemi operativi.

  I tipi di attacchi descritti di seguito risultano essere i più diffusi tra quelli che utilizzano le risorse di rete dei sistemi operativi:

  - *Attacchi di sovraccarico del buffer*: tipo di vulnerabilità del software determinata dall'incapacità o dalla totale assenza di controllo durante la gestione di grandi quantità di dati. Si tratta del tipo di vulnerabilità noto da più tempo e più semplice da sfruttare da parte degli hacker.
  - *Attacchi attraverso le stringhe di formato*: tipo di vulnerabilità nel software causata dal controllo insufficiente dei valori immessi per le funzioni I/O come printf(), fprintf(), scanf() e altre funzioni della libreria standard C. Se un programma presenta questa vulnerabilità, un hacker che riesce a inviare interrogazioni create con una tecnica speciale può assumere il controllo totale del sistema.

  Il Sistema di rilevamento intrusioni (vedere pagina 99) analizza automaticamente e impedisce i tentativi di sfruttare queste vulnerabilità nei servizi di rete più comuni (FTP, POP3, IMAP) se sono in esecuzione nel computer dell'utente.

  Gli *attacchi a Microsoft Windows* sfruttano le vulnerabilità nel software installato nel computer (ad esempio programmi come Microsoft SQL Server, Microsoft Internet Explorer, Messenger e componenti di sistema ai quali è possibile accedere attraverso la rete – DCom, SMB, Wins, LSASS, IIS5).

  Ad esempio, Anti-Hacker protegge il computer dagli attacchi che utilizzano le seguenti vulnerabilità di software note (questa lista di vulnerabilità è citata con il sistema di numerazione della Knowledge Base di Microsoft):

  (MS03-026) Vulnerabilità RPC DCOM (worm Lovesan)

  (MS03-043) Sovraccarico del buffer del servizio di Microsoft Messenger

  (MS03-051) Sovraccarico del buffer nelle estensioni del server di Microsoft FrontPage 2000

  (MS04-007) Vulnerabilità relativa a Microsoft Windows ASN.1

  (MS04-031) Sovraccarico remoto non autenticato del buffer del servizio Microsoft NetDDE

  (MS04-032) Sovraccarico heap per metafile (.emf) in Microsoft Windows XP

  (MS05-011) Gestione delle risposte di transazione del client SMB di Microsoft Windows

  (MS05-017) Vulnerabilità di sovraccarico del buffer del servizio accodamento messaggi di Microsoft Windows

  (MS05-039) Sovraccarico remoto del servizio Plug and Play di Microsoft Windows

  (MS04-045) Sovraccarico heap remoto del servizio Microsoft Windows Internet Naming (WINS)

  (MS05-051) Modifica della memoria del servizio Distributed Transaction Coordinator di Microsoft Windows

Esistono inoltre incidenti isolati di intrusioni mediante script dannosi, tra cui gli script elaborati da Microsoft Internet Explorer e i worm di tipo Helkern. Questo tipo di attacco consiste essenzialmente nell'invio di speciali pacchetti UDP a un computer remoto in grado di eseguire il codice dannoso.

Si tenga presente che, quando si è collegati alla rete, il computer è costantemente a rischio di attacchi da parte degli hacker. Per garantire la sicurezza del computer, accertarsi di abilitare il componente Anti-Hacker quando si naviga in Internet e aggiornare i database degli attacchi di rete a intervalli regolari (vedere la sezione "Selezione degli elementi da aggiornare" a pagina 141).

STATISTICHE DI ANTI-HACKER

Tutte le operazioni eseguite da Anti-Hacker vengono registrate in un rapporto. Le informazioni sulle attività eseguite dal componente sono raggruppate nelle seguenti schede:

- *Attacchi di rete* – questa scheda riporta l'elenco di tutti i tentativi di attacco di rete rilevati durante la sessione corrente di Kaspersky Anti-Virus.
- *Host vietati* – questa scheda riporta l'elenco di tutti gli host che sono stati bloccati per vari motivi, ad esempio per un tentativo d'attacco al computer o per l'intervento di una regola.
- *Attività applicazioni* – questa scheda visualizza le attività eseguite dalle applicazioni del computer.
- *Filtraggio pacchetti* – questa scheda riporta tutti i pacchetti di dati filtrati in base a una regola di Firewall.
- *Impostazioni* – in questa scheda si trovano le impostazioni seguite per l'esecuzione di Anti-Hacker.

Per visualizzare informazioni sulle attività del componente, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Rapporto** dal menu di scelta rapida del componente **Anti-Hacker**.

ANTI-SPAM

Kaspersky Anti-Virus include *Anti-Spam*, un componente che consente di rilevare messaggi indesiderati (spam) e di elaborarli in base alle regole del client di posta elettronica utilizzato, risparmiando tempo durante la gestione della posta.

Anti-Spam utilizza un algoritmo di autoaddestramento (vedere la sezione "Algoritmo di funzionamento del componente" a pag. 104), che consente di distinguere nel tempo tra spam e posta elettronica "valida" in maniera più accurata. L'origine dei dati per l'algoritmo viene estrapolata dal contenuto del messaggio. Per differenziare in maniera efficace spam e posta valida, Anti-Spam deve essere addestrato (vedere la sezione "Addestramento di Anti-Spam" a pag. 106).

Anti-Spam può essere utilizzato come plug-in dei client di posta seguenti:

- Microsoft Office Outlook.
- Microsoft Outlook Express (Windows Mail).
- The Bat!

Mediante la creazione di un elenco di indirizzi consentiti o bloccati, è possibile addestrare Anti-Spam a conoscere gli indirizzi che devono essere considerati "validi" per la provenienza dei messaggi e quelli da cui devono essere considerati spam. Inoltre, Anti-Spam è in grado di analizzare i messaggi alla ricerca di frasi contenute nell'elenco consentite e bloccate.

Anti-Spam consente di visualizzare i messaggi sul server ed eliminare quelli indesiderati senza scaricarli nel computer.

➡ *Per modificare le impostazioni di Anti-Spam, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, apportare le modifiche desiderate alle impostazioni del componente.

IN QUESTA SEZIONE

Algoritmo di funzionamento del componente 104

Addestramento di Anti-Spam 106

Modifica del livello di sensibilità 109

Filtraggio dei messaggi di posta sul server. Gestore della posta 109

Esclusione di messaggi di Microsoft Exchange Server dalla scansione 110

Selezione del metodo di scansione 111

Selezione della tecnologia di filtro anti-spam 111

Determinazione dei fattori di spam e probabile spam 112

Utilizzo delle funzioni avanzate di filtro anti-spam 112

Creazione dell'elenco di mittenti consentiti 113

Creazione dell'elenco di frasi consentite 114

Importazione dell'elenco di mittenti consentiti 114

Creazione dell'elenco di mittenti bloccati 115

Creazione dell'elenco di frasi bloccate 116

Azioni da eseguire con la posta spam 116

Ripristino delle impostazioni predefinite di Anti-Spam 120

Statistiche Anti-Spam 120

ALGORITMO DI FUNZIONAMENTO DEL COMPONENTE

Il funzionamento di Anti-Spam è suddiviso in due fasi:

- In primo luogo, Anti-Spam applica rigidi criteri per il filtro del messaggio. Tali criteri consentono di determinare con rapidità se il messaggio è spam o meno. Anti-Spam assegna al messaggio lo stato di *spam* o *non spam*, la scansione viene sospesa e il messaggio viene trasferito al client di posta per l'elaborazione (vedere i passaggi da 1 a 5 descritti di seguito).

- Nei passaggi successivi dell'algoritmo (da 6 a 10 in basso), Anti-Spam analizza i messaggi di posta elettronica che hanno superato i criteri di selezione precisi dei primi punti. Tali messaggi non possono essere inequivocabilmente considerati spam. Di conseguenza, Anti-Spam deve calcolare la *probabilità* che il messaggio appartenga alla categoria spam.

Di seguito, è riportata una descrizione dettagliata dell'algoritmo di funzionamento di Anti-Spam:

1. L'indirizzo del mittente viene analizzato alla ricerca di corrispondenze negli elenchi degli indirizzi bloccati e consentiti:

    - Se l'indirizzo di un mittente si trova nell'elenco dei mittenti consentiti, al messaggio verrà assegnato lo stato di *not spam*;

- Se l'indirizzo di un mittente si trova nell'elenco dei mittenti bloccati, al messaggio verrà assegnato lo stato di *spam*.

2. Se un messaggio è stato inviato mediante Microsoft Exchange Server e la scansione di tali messaggi è disabilitata, al messaggio verrà assegnato lo stato di *not spam*.

3. Il messaggio viene sottoposto all'analisi delle righe dell'elenco di frasi consentite. Se viene trovata almeno una riga inclusa in questo elenco, al messaggio viene assegnato lo stato *non spam*.

4. Il messaggio viene sottoposto all'analisi delle righe dell'elenco di frasi bloccate. Le probabilità che il messaggio sia spam aumentano se al suo interno vengono trovate parole incluse in questo elenco. Quando la probabilità calcolata supera il 100%, al messaggio verrà assegnato lo stato di *spam*.

5. Se il testo del messaggio contiene un indirizzo nel database di indirizzi Web sospetti e di phishing, il messaggio riceve lo stato di *spam*.

6. L'applicazione analizza i messaggi di posta elettronica tramite la tecnologia PDB. Durante questa operazione, Anti-Spam confronta le intestazioni dei messaggi di posta elettronica con i modelli di intestazioni dei messaggi spam. Ogni corrispondenza aumenta la probabilità che il messaggio sia effettivamente spam.

7. L'applicazione analizza i messaggi di posta elettronica tramite la tecnologia GSG. Durante questa operazione, Anti-Spam analizza le immagini allegate al messaggio di posta elettronica. Se l'analisi rileva la presenza di segni tipici di spam nell'oggetto allegato al messaggio, la probabilità che sia spam aumenta.

8. Anti-Spam analizza il messaggio di posta elettronica mediante la tecnologia Recent Terms. Durante questa operazione, Anti-Spam esegue la ricerca nel testo di frasi tipiche dello spam. Queste frasi sono contenute nei database aggiornabili di Anti-Spam. Una volta completata l'analisi, Anti-Spam calcola quanto è aumentata la probabilità che il messaggio sia spam.

9. Verifica la presenza delle funzioni avanzate (vedere la sezione "Utilizzo delle funzioni avanzate di filtraggio anti-spam" a pag. 112), tipiche dello spam. Ogni funzione rilevata aumenta la probabilità che il messaggio esaminato sia effettivamente spam.

10. Se Anti-Spam è stato addestrato, il messaggio viene analizzato tramite la tecnologia iBayes. L'algoritmo di autoaddestramento iBayes calcola la probabilità che un messaggio sia di tipo spam in base alla presenza di frasi tipiche dello spam nel testo del messaggio.

Il risultato dell'analisi del messaggio è la **probabilità** che quest'ultimo sia spam. I creatori di spam migliorano costantemente il mascheramento dello spam. Per questo motivo, nella maggior parte dei casi la probabilità calcolata non raggiunge il 100%. Per garantire un efficiente filtraggio dei messaggi di posta elettronica, Anti-Spam utilizza due parametri:

- *Fattore di spam* – il valore della probabilità che, se superato, fa sì che il messaggio venga considerato spam. Se la probabilità è inferiore a tale valore, ai messaggi viene assegnato lo stato di *probabile spam*.

- *Fattore di spam potenziale* – il valore della probabilità che, se superato, fa sì che il messaggio venga considerato spam potenziale. Se la probabilità è inferiore a tale valore, Anti-Spam considera il messaggio non spam.

In base ai fattori di spam e probabile spam specificati, ai messaggi viene assegnato lo stato *spam* o *probabile spam*. Ai messaggi verrà assegnata anche l'etichetta **[!! SPAM]** o **[!! Probable Spam]** nel campo dell'**Oggetto**. Successivamente, i messaggi vengono elaborati in base alle regole (vedere la sezione "Azioni da eseguire sui messaggi spam " a pag. 116) create per il client di posta.

VEDERE ANCHE

Anti-Spam..103

ADDESTRAMENTO DI ANTI-SPAM

Uno degli strumenti più potenti per il rilevamento dello spam è l'algoritmo iBayes di autoaddestramento. Questo algoritmo effettua una valutazione sullo stato del messaggio in base alle frasi in esso contenute. Prima di iniziare, è necessario inoltrare all'algoritmo iBayes alcune stringhe di esempio di posta utile e di posta spam a scopo di addestramento.

Esistono diversi approcci all'addestramento di Anti-Spam:

- Mediante l'addestramento guidato (vedere la sezione "Addestramento con Addestramento guidato" a pag. 106) (addestramento del pacchetto), consigliabile fin dal primo utilizzo di Anti-Spam.
- Addestramento di Anti-Spam mediante i messaggi in uscita (vedere la sezione "Addestramento tramite i messaggi di posta elettronica in uscita" a pag. 107).
- Addestramento diretto durante l'utilizzo della posta (vedere la sezione "Addestramento tramite il client di posta" a pag. 107) mediante i pulsanti speciali presenti sulla barra degli strumenti del client di posta o le voci di menu.
- Addestramento durante l'utilizzo dei rapporti di Anti-Spam (vedere la sezione "Addestramento con i rapporti" a pag. 108).

VEDERE ANCHE

Addestramento con Apprendimento guidato 106

Addestramento tramite i messaggi di posta elettronica in uscita 107

Addestramento tramite il client di posta 107

Addestramento con i rapporti 108

ADDESTRAMENTO CON APPRENDIMENTO GUIDATO

L'addestramento guidato può addestrare Anti-Spam (addestramento del pacchetto) indicando quali cartelle di posta elettronica contengono spam o messaggi validi.

Per il corretto riconoscimento dello spam è necessario utilizzare almeno 50 messaggi utili e 50 esempi di posta indesiderata. In caso contrario, l'algoritmo iBayes non funzionerà.

Per risparmiare tempo, l'Addestramento guidato limita l'addestramento a 50 messaggi tra quelli presenti in ciascuna cartella selezionata.

La procedura guidata è costituita da una serie di finestre (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Indietro** ed **Avanti**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

Per avviare l'addestramento guidato, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della sezione **Preparazione**, fare clic sul pulsante **Addestramento guidato**.

Quando si esegue l'addestramento in base a messaggi di posta elettronica validi, gli indirizzi dei mittenti dei messaggi vengono aggiunti all'elenco dei mittenti consentiti.

Per disabilitare l'aggiunta dell'indirizzo del mittente all'elenco dei mittenti consentiti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza** nella sezione Riservatezza.
5. Nella finestra visualizzata, sulla scheda **Elenco consentiti**, sezione **Mittenti consentiti**, deselezionare la casella **Aggiungi indirizzi dei mittenti consentiti durante l'addestramento Anti-Spam** nel client della posta.

ADDESTRAMENTO TRAMITE I MESSAGGI DI POSTA ELETTRONICA IN USCITA

È possibile addestrare Anti-Spam con un campione di 50 messaggi di posta in uscita. Gli indirizzi dei destinatari verranno aggiunti automaticamente all'elenco dei mittenti consentiti.

Per addestrare Anti-Spam con i messaggi in uscita:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Generale**, sezione **Posta in uscita**, selezionare la casella **Apprendimento mediante posta in uscita**.

Per disabilitare l'aggiunta dell'indirizzo del mittente all'elenco dei mittenti consentiti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, fare clic sul pulsante **Personalizza** nella sezione Riservatezza.
5. Nella finestra visualizzata, sulla scheda **Elenco consentiti**, sezione **Mittenti consentiti**, deselezionare la casella **Aggiungi indirizzi dei mittenti consentiti durante l'addestramento Anti-Spam** nel client della posta.

ADDESTRAMENTO TRAMITE IL CLIENT DI POSTA

L'addestramento mentre si gestiscono i messaggi di posta elettronica implica l'utilizzo di pulsanti speciali della barra degli strumenti del client di posta.

Per addestrare Anti-Spam tramite il client di posta, eseguire le seguenti operazioni:

1. Avviare il client di posta.

2. Selezionare un messaggio che si desidera utilizzare per l'addestramento di Anti-Spam.
3. Eseguire una delle azioni seguenti in base al client di posta in uso:
   - Premere il pulsante **Spam** o **Non spam** sulla barra degli strumenti di Microsoft Office Outlook.
   - Premere il pulsante **Spam** o **Non spam** sulla barra degli strumenti di Microsoft Outlook Express (Windows Mail).
   - Utilizzare le voci speciali **Contrassegna come spam** e **Contrassegna come non spam** del menu **Speciale** del programma del client di posta The Bat!.

Anti-Spam eseguirà l'addestramento mediante il messaggio selezionato. Se si selezionano più e-mail, l'addestramento avverrà sulla totalità di questi messaggi.

Se un messaggio viene contrassegnato come non spam, l'indirizzo del relativo mittente verrà aggiunto all'elenco dei mittenti consentiti.

Per disabilitare l'aggiunta dell'indirizzo del mittente all'elenco dei mittenti consentiti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda Elenco consentiti, nella sezione **Mittenti consentiti**, deselezionare la casella **Includi gli indirizzi dei mittenti consentiti nell'addestramento Anti-Spam del client di posta**.

Se è necessario selezionare più messaggi contemporaneamente o si è certi che una cartella contenga solo messaggi di un unico gruppo (spam o non spam), è possibile adottare un approccio più complesso all'addestramento utilizzando l'addestramento guidato.

ADDESTRAMENTO CON I RAPPORTI

È possibile scegliere di addestrare Anti-Spam in base ai rapporti. I rapporti del componente, infatti, consentono di valutare l'accuratezza della configurazione e, se necessario, di apportare determinate correzioni ad Anti-Spam.

Per contrassegnare un determinato messaggio come spam o non spam, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Rapporto** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della scheda **Eventi**, selezionare il messaggio che si desidera utilizzare come base per l'addestramento avanzato.
5. Selezionare una della azioni seguenti dal menu di scelta rapida del messaggio:
   - **Contrassegna come spam**.
   - **Contrassegna come non spam**.
   - **Aggiungi all'Elenco Consentiti**.

- **Aggiungi all'Elenco Bloccati**.

MODIFICA DEL LIVELLO DI SENSIBILITÀ

Kaspersky Anti-Virus 6.0 per Windows Workstations MP4 protegge dallo spam a uno dei seguenti livelli:

- **Blocca tutti –** il più alto livello di protezione in cui qualsiasi messaggio viene considerato spam tranne quelli contenenti righe dall'elenco delle frasi consentite e i cui mittenti sono inclusi nell'elenco degli indirizzi consentiti. Tutte le altre funzioni sono disabilitate.

- **Alto** – livello alto che, se attivato, aumento le probabilità che alcuni messaggi non spam, verranno contrassegnati come *spam*. A questo livello, il messaggio viene analizzato mediante gli indirizzi e le frasi consentiti e bloccati, e quindi mediante le tecnologie PDB e GSG e l'algoritmo iBayes.

  Questo livello deve essere applicato quando esiste un'elevata probabilità che l'indirizzo del destinatario sia ignorato dagli spammer. Ad esempio, quando il destinatario non è registrato in messaggi di massa e non dispone di un indirizzo di posta elettronica su server di posta gratuiti/non aziendali.

- **Consigliato –** il livello di impostazioni più comune per la classificazione dei messaggi di posta elettronica.

  Con questo livello è possibile che alcuni messaggi spam non vengano rilevati. Ciò avviene quando Anti-Spam non è stato configurato alla perfezione. Si consiglia di condurre un addestramento avanzato del modulo mediante l'addestramento guidato o i pulsanti **Spam** / **Not Spam** (voci di menu in The Bat!), utilizzando lettere spam non rilevate.

- **Basso** – livello di impostazioni meno restrittivo. Può essere consigliato nel caso di corrispondenza che contenga un elevato numero di parole riconosciute da Anti-Spam come spam, pur trattandosi di messaggi validi. La causa di questo tipo di situazione può essere legata alla professione del destinatario, il quale è costretto a utilizzare termini specifici nella sua corrispondenza lavorativa che risultano diffusi nello spam. In questo livello vengono utilizzate tutte le tecnologie di rilevamento dello spam per analizzare la posta elettronica.

- **Consenti tutti** – il più basso livello di sensibilità in cui sono considerati spam solo i messaggi contenenti righe presenti nell'elenco delle frasi bloccate e i cui mittenti sono inclusi nell'elenco degli indirizzi bloccati. Tutte le altre funzioni sono disabilitate.

Per impostazione predefinita, la protezione anti-spam è impostata al livello di riservatezza **Consigliato**. È possibile aumentare o ridurre il livello o modificare le impostazioni del livello corrente.

➧ *Per modificare il livello di sensibilità selezionato del componente Anti-Spam, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, spostare la barra del cursore lungo la gradazione del livello di sensibilità. Regolando il livello di sensibilità, è possibile definire la correlazione tra i fattori di spam, spam probabile e posta valida.

FILTRO DEI MESSAGGI DI POSTA SUL SERVER. GESTORE DELLA POSTA

Recapito posta è progettato per la visualizzazione dei messaggi di posta sul server senza scaricarli nel computer. Questo consente di rifiutare alcuni messaggi in modo da risparmiare tempo, ridurre il traffico durante l'utilizzo della posta e diminuire inoltre il rischio di scaricare spam o virus nel computer.

Per gestire i messaggi presenti sul server viene utilizzato il componente **Recapito posta**. La finestra del gestore della posta viene visualizzata sempre prima del recupero della posta, a condizione che il componente sia abilitato.

Recapito posta viene avviato solo se la posta viene ricevuta tramite POP3. Tale componente non viene visualizzato se il server POP3 non supporta la visualizzazione delle intestazioni dei messaggi o se tutti i messaggi nel server provengono da indirizzi inclusi nell'elenco di mittenti consentiti.

L'elenco di messaggi presenti sul server viene visualizzato nella parte centrale della finestra di Recapito posta. Selezionare il messaggio nell'elenco per analizzarne in modo dettagliato l'intestazione. La visualizzazione dell'intestazione può risultare utile, ad esempio, nella situazione seguente. Gli spammer installano un programma dannoso nel computer di un collega dell'utente. Tale programma invia messaggi spam che includono il suo nome, utilizzando l'elenco contatti del suo client di posta. La probabilità che il proprio indirizzo sia presente nell'elenco contatti del collega è piuttosto elevata. È quasi certo dunque che la propria casella di posta verrà riempita di messaggi spam. In questi casi non è possibile stabilire se un messaggio è stato inviato dal collega o da uno spammer utilizzando solo l'indirizzo del mittente. È necessario utilizzare le intestazioni dei messaggi! Verificare con attenzione il mittente, la data e le dimensioni del messaggio. Monitorare il percorso del messaggio dal mittente al server di posta. Tutte queste informazioni dovrebbero essere presenti nelle intestazioni. Valutare se è realmente necessario scaricare il messaggio dal server o se è meglio eliminarlo.

➧ *Per utilizzare Recapito posta, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Generale**, selezionare la casella ☑ **Apri Recapito posta alla ricezione della posta attraverso POP3**.

➧ *Per eliminare i messaggi dal server mediante Recapito posta, eseguire le seguenti operazioni:*

1. Selezionare la casella accanto al messagio nella colonna **Elimina** della finestra del gestore della posta.
2. Premere il pulsante **Elimina selezionati** nella parte superiore della finestra.

I messaggi verranno eliminati dal server. Verrà ricevuta una notifica contrassegnata come **[!! SPAM]** ed elaborata in base alle regole impostate per il client di posta in uso.

ESCLUSIONE DI MESSAGGI DI MICROSOFT EXCHANGE SERVER DALLA SCANSIONE

È possibile escludere dalla scansione anti-spam i messaggi di posta elettronica provenienti dalla rete interna, ad esempio la posta aziendale. Tenere presente che tali messaggi verranno considerati come posta interna se si utilizza Microsoft Office Outlook in tutti i computer di rete e le caselle di posta degli utenti si trovano sullo stesso server di Exchange o su server collegati mediante connettori X400.

Per impostazione predefinita, Anti-Spam non esamina i messaggi di Microsoft Exchange Server.

➧ *Se si desidera che Anti-Spam analizzi i messaggi, eseguire le seguenti operazioni:*

1. Aprire nella finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.

5. Nella finestra visualizzata, all'interno della scheda **Generale**, deselezionare la casella **Non controllare messaggi nativi di Microsoft Exchange Server**.

SELEZIONE DEL METODO DI SCANSIONE

I metodi di scansione consentono la verifica dei collegamenti all'interno dei messaggi di posta elettronica per rilevare se sono inclusi nell'elenco di indirizzi Web sospetti e/o nell'elenco di indirizzi di phishing.

Il controllo che tali collegamenti non siano inclusi nell'elenco di indirizzi di phishing consente di evitare attacchi di phishing, che si presentano sotto forma di messaggi di posta elettronica provenienti da sedicenti istituti finanziari contenenti collegamenti ai relativi siti Web. Il testo del messaggio induce il lettore a cliccare sul collegamento e a immettere informazioni riservate nella finestra che segue, ad esempio, un numero di carta di credito o il nome utente e la password usati per collegarsi al proprio sito di Internet banking per eseguire operazioni finanziarie.

Un attacco di phishing può essere occultato, ad esempio, sotto forma di lettera proveniente dalla propria banca con un collegamento al relativo sito Web ufficiale. Facendo clic sul collegamento, si arriva a una copia identica del sito della banca che visualizza addirittura l'indirizzo effettivo nel browser, anche se in realtà di tratta di un sito falso. Da questo momento in poi, tutte le operazioni eseguite nel sito possono essere ricostruite e utilizzate per prelevare denaro dal conto dell'utente.

Per eseguire la scansione dei collegamenti nei messaggi utilizzando il database di indirizzi sospetti, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Generale**, selezionare la casella **Confronta gli URL con il database degli indirizzi sospetti**.

Per eseguire la scansione dei collegamenti nei messaggi utilizzando il database di indirizzi di phishing, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Generale**, selezionare la casella **Confronta gli URL con il database degli indirizzi di phishing**.

SELEZIONE DELLA TECNOLOGIA DI FILTRO ANTI-SPAM

I messaggi di posta elettronica vengono sottoposto a scansione anti-spam mediante tecnologie di filtro avanzate.

Per impostazione predefinita, il programma utilizza tutte le tecnologie di filtro, garantendo la più completa analisi dei messaggi di posta elettronica.

Per disabilitare qualunque tecnologia di filtro:

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Algoritmi**, sezione **Algoritmi di riconoscimento**, deselezionare le caselle ☑ relative alle tecnologie di filtro che non si desidera utilizzare per l'analisi anti-spam dei messaggi di posta elettronica.

DETERMINAZIONE DEI FATTORI DI SPAM E PROBABILE SPAM

Gli specialisti di Kaspersky Lab si sono impegnati al meglio per configurare in maniera ottimale Anti-Spam per la rilevazione di spam e spam potenziale.

Le operazioni di rilevamento dello spam basate sulle tecnologie di filtro all'avanguardia consentono di addestrare Anti-Spam per l'identificazione accurata dello spam, del probabile spam e della posta valida con un determinato numero di messaggi della Posta in arrivo.

La configurazione dello strumento Anti-Spam può essere eseguita utilizzando l'Apprendimento guidato e sulla base dei messaggi elaborati dai client di posta elettronica. Così facendo, a ogni singolo elemento dei messaggi di posta elettronica utili o dei messaggi spam viene assegnato un fattore. Quando un messaggio di posta elettronica entra a far parte della cartella della posta in arrivo, Anti-Spam lo analizza utilizzando l'algoritmo iBayes per distinguere tra spam e messaggi validi. I fattori di ciascun elemento vengono sommati e viene quindi calcolato un fattore di spam e un fattore di probabile spam.

Il fattore di probabile spam definisce un limite al di sopra del quale il messaggio di posta elettronica verrà classificato come probabile spam. Se si utilizza il livello di sensibilità **Consigliato** di Anti-Spam, tutti i messaggi di posta elettronica con fattore compreso tra 50% e 59% verranno considerati probabile spam. Per posta valida si intendono quei messaggi che dopo la scansione presentano un fattore di spam minore di 50%.

Il fattore di spam definisce un limite al di sopra del quale il messaggio di posta elettronica verrà classificato come spam. Qualsiasi messaggio il cui fattore abbia un valore superiore a quello specificato verrà considerato spam. Per impostazione predefinita, il fattore di spam è pari al 59% per il livello **Consigliato**. Questo significa che qualsiasi messaggio il cui fattore abbia un valore superiore al 59% verrà contrassegnato come spam.

➡ *Per modificare le impostazioni di Anti-Spam, eseguire le operazioni seguenti:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Algoritmi** impostare i fattori di spam e spam probabile nelle sezioni appropriate.

UTILIZZO DELLE FUNZIONI AVANZATE DI FILTRO ANTI-SPAM

Oltre alle funzioni principali utilizzate per filtrare lo spam (creazione di elenchi di elementi consentiti ed elementi bloccati, analisi mediante tecnologie di filtro), è possibile impostare funzioni avanzate. In base a tali funzioni, a un messaggio verrà assegnato lo stato di **spam** con un determinato grado di probabilità.

I messaggi spam potrebbero essere e-mail vuote (senza oggetto o corpo del messaggio), e-mail contenenti collegamenti a immagini o con immagini incorporate, con il testo in caratteri molto piccoli. Lo spam può essere costituito da e-mail con caratteri invisibili (con il testo uguale al colore di sfondo), e-mail contenenti elementi nascosti (elementi non visualizzati) oppure tag HTML non corretti e e-mail contenenti script (serie di istruzioni eseguite all'apertura dell'e-mail).

Per configurare le funzioni avanzate del filtro anti-spam, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione .
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.
5. Nella finestra visualizzata, all'interno della scheda **Algoritmi**, fare clic sul pulsante **Avanzate**.
6. Nella finestra **Avanzate** visualizzata, selezionare le caselle relative ai segni di spam scelti. Per le funzioni avanzate incluse, specificare il fattore di spam (in percentuale) che stabilirà la probabilità di classificazione di un messaggio come spam. Il valore predefinito del fattore di spam è 80%.

   Il valore di probabilità di spam calcolato grazie all'utilizzo di funzioni avanzate del filtro di spam viene aggiunto alla valutazione generale restituita all'intero messaggio tramite Anti-Spam.

   Se si abilita il filtro basato sulla funzione di incremento del fattore di spam per i messaggi non inviati espressamente all'utente ("increase spam factor for messages not sent specifically to me"), è necessario specificare l'elenco degli indirizzi di posta elettronica attendibili. A tale scopo, premere il pulsante **Indirizzi personali**. Nella finestra **Indirizzi personali** visualizzata, specificare l'elenco di indirizzi e di maschere di indirizzi. Quando esegue la scansione di un messaggi, Anti-Spam verifica anche l'indirizzo del destinatario. Se l'indirizzo non corrisponde a uno di quelli presenti nell'elenco, al messaggio di posta elettronica verrà etichettato come **spam**.

CREAZIONE DELL'ELENCO DI MITTENTI CONSENTITI

L'elenco di indirizzi consentiti contiene gli indirizzi dei mittenti dai quali si ritiene non verrà ricevuto spam. Tale elenco viene riempito automaticamente durante l'addestramento del componente Anti-Spam. L'elenco può essere modificato.

L'elenco può contenere indirizzi o maschere di indirizzi. Le maschere supportano l'utilizzo dei caratteri jolly standard ***** e **?**, dove ***** rappresenta una qualsiasi combinazione di caratteri e **?** indica un singolo carattere. Esempi di maschere di indirizzi:

- *ivanov@test.ru*: i messaggi provenienti da questo indirizzo verranno sempre classificati come validi;
- **@test.ru:* la posta proveniente da qualsiasi mittente del dominio di posta test.ru mail verrà sempre considerata come valida, ad esempio, *petrov@test.ru*, *sidorov@test.ru*;
- *ivanov@:* la posta proveniente dal mittente con lo stesso nome, indipendentemente dal dominio di posta, verrà sempre considerata come valida, ad esempio *ivanov@test.ru*, *ivanov@mail.ru*;
- **@test:* la posta proveniente da qualsiasi mittente da un dominio di posta che inizia con *test* non verrà considerata come spam, ad esempio *ivanov@test.ru*, *petrov@test.com*;
- *ivan.*@test.???* : le e-mail provenienti da un mittente, il cui nome inizia con *ivan.* e il cui nome di dominio di posta inizia con *test* e termina con tre caratteri qualsiasi, non verrà mai considerata come spam, ad esempio *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

Per creare un elenco di mittenti consentiti, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.

4. Nella finestra visualizzata, sulla scheda **Elenco consentiti**, sezione **Mittenti consentiti**, selezionare la casella **Considera messaggi di posta elettronica provenienti dai seguenti mittenti come non spam**, quindi cliccare sul pulsante **Aggiungi**.

5. Nella finestra **Maschera indirizzi e-mail** visualizzata, immettere l'indirizzo o la maschera necessari.

CREAZIONE DELL'ELENCO DI FRASI CONSENTITE

L'elenco di frasi consentite contiene frasi di messaggi chiave contrassegnate come non spam e può essere creato dall'utente.

Per definire le frasi è anche possibile utilizzare le maschere. Durante la creazione di una maschera, le maschere supportano l'utilizzo dei caratteri jolly standard ***** e **?**, dove ***** rappresenta una qualsiasi combinazione di caratteri e **?** indica un singolo carattere. Esempi di frasi e maschere di frasi:

- *Ciao Ivan!* : un messaggio di posta elettronica contenente solo questo testo è considerato come posta valida. L'utilizzo di righe simili alle seguenti è sconsigliato.
- *Ciao Ivan!**: un messaggio di posta elettronica che inizia con la frase *Ciao Ivan!* è considerato come posta valida.
- *Ciao *! **: i messaggi di posta elettronica che iniziano con il saluto *Ciao* e un punto esclamativo ovunque nel messaggio non vengono considerati come spam.
- ** Ivan? *:* i messaggi di posta elettronica che iniziano con l'indirizzo personale *Ivan* seguito da qualsiasi carattere non vengono considerati come spam.
- ** Ivan\? *:* i messaggi di posta elettronica che contengono la frase *Ivan?* sono considerati come validi.

Se in una frase sono inclusi i caratteri * e ?, è necessario farli precedere dal carattere \ per impedire che vengano interpretati erroneamente in Anti-Spam. Quindi, vengono utilizzati due caratteri anziché uno: * e \?.

Per creare l'elenco di frasi consentite:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Elenco consentiti**, sezione **Frasi consentiti**, selezionare la casella **Considera messaggi di posta elettronica contenenti le seguenti locuzioni come non spam**, quindi cliccare sul pulsante **Aggiungi**.
6. Nella finestra **Frase consentita** visualizzata, immettere una riga o una maschera.

IMPORTAZIONE DELL'ELENCO DI MITTENTI CONSENTITI

Gli indirizzi contenuti nell'elenco di mittenti consentiti possono essere importati dai file *.txt*, *.csv* o dalla rubrica di Microsoft Office Outlook/Microsoft Outlook Express.

Per importare un elenco di mittenti consentiti, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.

4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.

5. Nella finestra visualizzata, sulla scheda **Elenco consentiti**, sezione **Mittenti consentiti**, cliccare sul pulsante **Importa**.

6. Selezionare l'origine di importazione dal menu a discesa:

   - Se è stata selezionata la voce **Dal file**, verrà visualizzata la finestra di selezione. L'applicazione supporta l'importazione da file di tipo *.csv* o *.txt*.

   - Se è stata selezionata la voce **Dalla rubrica indirizzi**, verrà visualizzata la finestra di selezione della rubrica. Selezionare la rubrica desiderata da questa finestra.

CREAZIONE DELL'ELENCO DI MITTENTI BLOCCATI

L'elenco di mittenti bloccati contiene gli indirizzi dei mittenti dei messaggi contrassegnati come spam. Tale elenco viene compilato manualmente.

L'elenco può contenere indirizzi o maschere di indirizzi. Le maschere supportano l'utilizzo dei caratteri jolly standard ***** e **?**, dove ***** rappresenta una qualsiasi combinazione di caratteri e **?** indica un singolo carattere. Esempi di maschere di indirizzi:

- *ivanov@test.ru*: i messaggi provenienti da questo indirizzo verranno sempre classificati come spam;

- **@test.ru:* la posta proveniente da qualsiasi mittente del dominio di posta *test.ru* mail verrà sempre classificata come spam, ad esempio, *petrov@test.ru*, *sidorov@test.ru*;

- *ivanov@:* la posta proveniente dal mittente con lo stesso nome, indipendentemente dal dominio di posta, verrà sempre considerata come spam, ad esempio *ivanov@test.ru*, *ivanov@mail.ru*;

- **@test:* la posta proveniente da qualsiasi mittente da un dominio di posta che inizia con *test* verrà considerata come spam, ad esempio *ivanov@test.ru*, *petrov@test.com*;

- *ivan.*@test.???* : le e-mail provenienti da un mittente, il cui nome inizia con *ivan.* e il cui nome di dominio di posta inizia con *test* e termina con tre caratteri qualsiasi, non verrà mai considerata come spam, ad esempio *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

Per creare un elenco di mittenti bloccati, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.

3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.

4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.

5. Nella finestra visualizzata, sulla scheda **Elenco bloccati**, sezione **Mittenti consentiti**, selezionare la casella ☑ **Considera e-mail provenienti dai seguenti mittenti come spam**, quindi cliccare sul pulsante **Aggiungi**.

6. Nella finestra **Maschera indirizzi e-mail** visualizzata, immettere l'indirizzo o la maschera necessari.

CREAZIONE DELL'ELENCO DI FRASI BLOCCATE

Nell'elenco di mittenti bloccati vengono archiviate frasi chiave dai messaggi di posta elettronica contrassegnati come spam. Tale elenco viene compilato manualmente.

Per definire le frasi è anche possibile utilizzare le maschere. Durante la creazione di una maschera, le maschere supportano l'utilizzo dei caratteri jolly standard ***** e **?**, dove ***** rappresenta una qualsiasi combinazione di caratteri e ? indica un singolo carattere. Esempi di frasi e maschere di frasi:

- *Ciao Ivan!* : un messaggio di posta elettronica contenente solo questo testo è considerato come spam. Si consiglia di non utilizzare questa frase come frase da elencare.
- *Ciao Ivan!**: un messaggio di posta elettronica che inizia con la frase *Ciao Ivan!* verrà considerato come spam.
- *Ciao *! *:* un messaggio di posta elettronica che inizia con *Ciao* e un punto esclamativo in qualsiasi parte del messaggio verrà considerato come spam.
- ** Ivan? *:* un messaggio di posta elettronica che contiene un saluto a un utente con il nome *Ivan* il cui nome è seguito da qualsiasi carattere verrà considerato come spam.
- ** Ivan\? *:* un messaggio di posta elettronica che contiene la frase *Ivan?* viene considerato come spam.

Se in una frase sono inclusi i caratteri * e ?, è necessario farli precedere dal carattere \ per impedire che vengano interpretati erroneamente in Anti-Spam. Quindi, vengono utilizzati due caratteri anziché uno: * e \?.

Durante la scansione di un messaggio di posta elettronica, i relativi contenuti vengono analizzati in Anti-Spam a fronte delle stringhe contenute nell'elenco bloccati. Le probabilità che il messaggio sia spam aumentano se al suo interno vengono trovate parole incluse in questo elenco. Quando la probabilità calcolata supera il 100%, al messaggio verrà assegnato lo stato di *spam*.

Per creare l'elenco di frasi bloccate:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, all'interno della sezione **Riservatezza**, premere il pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Frasi bloccate**, sezione **Mittenti consentiti**, selezionare la casella ☑ **Considera messaggi di posta elettronica contenenti le seguenti locuzioni come spam**, quindi cliccare sul pulsante **Aggiungi**.
6. Nella finestra **Frase bloccata** visualizzata, immettere una riga o una maschera.

AZIONI DA ESEGUIRE CON LA POSTA SPAM

Se in seguito alla scansione vengono identificati messaggi contenenti spam o probabile spam, le azioni successive di Anti-Spam dipendono dallo stato dell'oggetto e dall'azione selezionata. Per impostazione predefinita, i messaggi di posta classificati come *spam* o *probabile spam* vengono modificati mediante l'aggiunta rispettivamente dell'etichetta **[!! SPAM]** o **[?? Probable Spam]** nel campo **Oggetto** del messaggio.

È possibile selezionare azioni supplementari da intraprendere sui messaggi classificati come spam o probabile spam. A tale scopo, vengono forniti plug-in speciali nei client Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail) e The Bat!. Per gli altri client di posta, è possibile configurare le regole di filtraggio.

VEDERE ANCHE

Configurazione dell'elaborazione della posta spam in Microsoft Office Outlook 117

Configurazione dell'elaborazione della posta spam in Microsoft Outlook Express (Windows Mail) 118

Configurazione dell'elaborazione della posta spam in The Bat! 119

CONFIGURAZIONE DELL'ELABORAZIONE DELLA POSTA SPAM IN MICROSOFT OFFICE OUTLOOK

La finestra relativa alle impostazioni dell'elaborazione della posta spam viene visualizzata automaticamente alla prima esecuzione del client di posta dopo aver installato l'applicazione.

Per impostazione predefinita, i messaggi di posta elettronica classificati da Anti-Spam come *spam* o *probabile spam* sono segnalati da etichette speciali, **[!! SPAM]** o **[?? Probable Spam]**, nel campo **Oggetto**.

Ai messaggi classificati come spam e probabile spam è possibile applicare le regole di elaborazione seguenti:

- **Sposta nella cartella**: il messaggio spam viene spostato nella cartella della casella di posta in arrivo specificata.
- **Copia nella cartella**: il messaggio di posta elettronica viene copiato e spostato nella cartella specificata. Il messaggio di posta elettronica originale viene salvato nella **Posta in arrivo**.
- **Elimina**: il messaggio spam viene eliminato dalla casella di posta dell'utente.
- **Ignora**: il messaggio di posta elettronica rimane nella cartella della **Posta in arrivo**.

A questo scopo, selezionare il valore appropriato nell'elenco a discesa nella sezione **Spam** o **Probabile spam**.

Ulteriori azioni disponibili per la gestione della posta spam e probabile spam in Microsoft Office Outlook sono disponibili sulla scheda speciale **Anti-Spam** nel menu **Strumenti** → **Opzioni**.

Visualizzata automaticamente quando il client di posta viene aperto per la prima volta dopo aver installato l'applicazione e in cui si richiede se si desidera configurare l'elaborazione della posta spam.

Durante l'addestramento di Anti-Spam tramite il client di posta, un messaggio contrassegnato viene inviato a Kaspersky Lab come esempio di spam. Cliccare sul collegamento **Azione aggiuntiva da eseguire dopo aver contrassegnato manualmente i messaggi come spam** per selezionare la modalità di trasferimento dello spam di esempio nella finestra visualizzata.

È inoltre possibile selezionare l'algoritmo per il funzionamento standard di Microsoft Office Outlook e del plug-in Anti-Spam:

- **Scansione alla ricezione**. Tutti i messaggi di posta elettronica che arrivano nella cartella Posta in arrivo dell'utente vengono inizialmente elaborati in base alle regole di Microsoft Office Outlook. Al termine dell'elaborazione, i messaggi rimanenti che non rientrano in alcuna regola vengono elaborati dal plug-in Anti-Spam. In altre parole, i messaggi vengono elaborati in base alla priorità delle regole. Talvolta, la sequenza di priorità può essere ignorata se, ad esempio, nella Posta in arrivo giungono contemporaneamente molti messaggi. Di conseguenza, possono verificarsi casi in cui informazioni su un messaggio di posta elettronica elaborato da una regola di Microsoft Office Outlook vengono registrate nel rapporto Anti-Spam contrassegnato con lo stato *spam*. Per evitare che ciò accada, si consiglia di configurare il plug-in Anti-Spam come una regola di Microsoft Outlook.
- **Usa Regola di Microsoft Office Outlook**. Questa opzione consente di elaborare i messaggi in entrata mediante la gerarchia delle regole di Microsoft Office Outlook, una delle quali dovrebbe corrispondere alla regola di elaborazione dei messaggi di posta elettronica in Anti-Spam. Si tratta della configurazione migliore in

quanto non causa conflitti tra Microsoft Outlook e il plug-in Anti-Spam. L'unico inconveniente è la necessità di creare ed eliminare manualmente le regole di elaborazione dello spam attraverso Microsoft Office Outlook.

Per creare una regola di elaborazione della posta spam, eseguire le seguenti operazioni:

1. Eseguire Microsoft Office Outlook e utilizzare il comando **Strumenti** → **Regole e avvisi** nel menu principale dell'applicazione. Il comando per l'apertura dello strumento varia in base alla versione di Microsoft Office Outlook. In questo file della Guida viene illustrato come creare una regola utilizzando Microsoft Office Outlook 2003.
2. Nella finestra **Regole e avvisi** visualizzata, scheda **Regole posta elettronica**, cliccare sul pulsante **Nuova regola**. Verrà avviata la Creazione guidata Regole, che include i passaggi seguenti:
   a. Scegliere se creare una regola ex novo o utilizzando un modello. Selezionare l'opzione **Crea nuova regola** e selezionare la condizione di scansione **Controlla messaggi in arrivo**. Cliccare sul pulsante **Avanti**.
   b. Premere il pulsante **Avanti** nella finestra di configurazione delle condizioni di filtraggio dei messaggi senza selezionare alcuna casella. Nella finestra di dialogo, confermare che si desidera applicare questa regola a tutti i messaggi ricevuti.
   c. Nella finestra di selezione delle azioni da applicare ai messaggi, selezionare la casella ☑ **Esegui un'azione personalizzata** nell'elenco di azioni. Nella parte inferiore della finestra, cliccare sul collegamento **un'azione personalizzata**. Selezionare **Kaspersky Anti-Spam** dal menu a discesa nella finestra visualizzata, quindi cliccare sul pulsante **OK**.
   d. Premere il pulsante **Avanti** nella finestra delle esclusioni dalla regola senza selezionare alcuna casella.
   e. Nell'ultima finestra è possibile modificare il nome delle regola (quello predefinito è **Kaspersky Anti-Spam**). Verificare che la casella ☑ **Attiva regola** sia selezionata e premere il pulsante **Fine**.
3. Per impostazione predefinita, la nuova regola viene posizionata all'inizio dell'elenco di regole nella finestra **Regole e avvisi**. Se si desidera, è possibile spostarla alla fine dell'elenco in modo che venga applicata per ultima ai messaggi di posta elettronica.

Tutti i messaggi di posta elettronica in arrivo vengono elaborati in base a queste regole. L'ordine in cui il programma applica le regole ai messaggi di posta elettronica dipende dalla priorità assegnata a ciascuna di esse. Le regole vengono applicate a partire dall'inizio dell'elenco. Ogni regola successiva viene classificata con una priorità inferiore rispetto alla precedente. È possibile modificare la priorità di applicazione delle regole ai messaggi.

Se non si desidera che la regola Anti-Spam elabori ulteriormente i messaggi di posta elettronica dopo l'applicazione di una regola, si consiglia di selezionare la casella ☑ **Interrompi l'elaborazione di ulteriori regole** nelle impostazioni delle regole (vedere il passaggio 3 della procedura di creazione delle regole).

Se si ha esperienza nella creazione di regole per l'elaborazione della posta in Microsoft Outlook, è possibile creare regole personalizzate per Anti-Spam in base all'algoritmo suggerito.

VEDERE ANCHE

Configurazione dell'elaborazione della posta spam in Microsoft Outlook Express (Windows Mail)............................... 118

Configurazione dell'elaborazione della posta spam in The Bat! 119

CONFIGURAZIONE DELL'ELABORAZIONE DELLA POSTA SPAM IN MICROSOFT OUTLOOK EXPRESS (WINDOWS MAIL)

La finestra delle impostazioni di elaborazione dello spam viene aperta quando si esegue il client dopo aver installato l'applicazione.

Per impostazione predefinita, i messaggi di posta elettronica classificati da Anti-Spam come *spam* o *probabile spam* sono segnalati da etichette speciali, **[!! SPAM]** o **[?? Probable Spam]**, nel campo **Oggetto**.

Ulteriori azioni eseguibili sulla posta spam e probabile spam in Microsoft Outlook Express (Windows Mail) sono disponibili in una finestra speciale visualizzata quando si clicca sul pulsante **Impostazioni** accanto agli altri bottoni di Anti-Spam, **Spam** e **Non spam**, sulla barra delle applicazioni.

Tale finestra viene visualizzata automaticamente quando il client di posta viene aperto per la prima volta dopo aver installato l'applicazione e in cui si richiede se si desidera configurare l'elaborazione della posta spam.

Ai messaggi classificati come spam e probabile spam è possibile applicare le regole di elaborazione seguenti:

- **Sposta nella cartella**: il messaggio spam viene spostato nella cartella della casella di posta in arrivo specificata.
- **Copia nella cartella**: il messaggio di posta elettronica viene copiato e spostato nella cartella specificata. Il messaggio di posta elettronica originale viene salvato nella **Posta in arrivo**.
- **Elimina**: il messaggio spam viene eliminato dalla casella di posta dell'utente.
- **Ignora**: il messaggio di posta elettronica rimane nella cartella della **Posta in arrivo**.

A questo scopo, selezionare il valore appropriato nell'elenco a discesa nella sezione **Spam** o **Probabile spam**.

Durante l'addestramento di Anti-Spam tramite il client di posta, un messaggio contrassegnato viene inviato a Kaspersky Lab come esempio di spam. Cliccare sul collegamento **Azione aggiuntiva da eseguire dopo aver contrassegnato manualmente i messaggi come spam** per selezionare la modalità di trasferimento dello spam di esempio nella finestra visualizzata.

Le impostazioni per l'elaborazione della posta spam vengono archiviate come regole di Microsoft Outlook Express (Windows Mail). Di conseguenza, per salvare le modifiche, è necessario riavviare Microsoft Outlook Express (Windows Mail).

VEDERE ANCHE

Configurazione dell'elaborazione della posta spam in Microsoft Office Outlook 117

Configurazione dell'elaborazione della posta spam in The Bat! 119

CONFIGURAZIONE DELL'ELABORAZIONE DELLA POSTA SPAM IN THE BAT!

Le azioni da eseguire in caso di spam e probabile spam in The Bat! sono definite dagli strumenti del client.

Per impostare le regole di elaborazione dello spam in The Bat!, eseguire le operazioni seguenti:

1. Selezionare **Impostazioni** dal menu **Proprietà** del client di posta.
2. Selezionare **Protezione spam** nella struttura ad albero delle impostazioni.

Le impostazioni visualizzate della protezione anti-spam sono applicabili a tutti i moduli Anti-Spam installati che supportano l'integrazione con The Bat!.

Si consiglia di impostare il livello di classificazione e specificare le modalità di risposta ai messaggi con una determinata classificazione (nel caso di Anti-Spam, la classificazione rappresenta la probabilità che il messaggio di posta elettronica sia spam):

- Eliminare i messaggi con una classificazione superiore al livello specificato;
- Trasferire i messaggi di posta con un determinato fattore in una cartella destinata allo spam;
- Trasferire nella cartella dello spam i messaggi classificati come spam con intestazioni speciali;
- Lasciare lo spam nella cartella **Posta in arrivo**.

Dopo aver elaborato un messaggio, Kaspersky Anti-Virus assegna ad esso lo stato di spam o probabile spam in base a un fattore con valore regolabile. The Bat! dispone di un algoritmo di classificazione dei messaggi personalizzato, anch'esso basato su un fattore di spam. Per quanto riguarda il fattore di spam i cui i valori corrispondono in Kaspersky Anti-Virus e in The Bat!, a tutti i messaggi verificati da Anti-Spam viene assegnata una classificazione, in base allo stato del messaggio: posta valida – 0%, probabile spam – 50%, spam – 100%. Pertanto, la classificazione della posta di The Bat! corrisponde al fattore dello stato correlato e non al fattore della posta assegnato in Anti-Spam.

Per ulteriori informazioni sulle regole di classificazione e di elaborazione dello spam, consultare la documentazione relativa a The Bat!.

VEDERE ANCHE

Configurazione dell'elaborazione della posta spam in Microsoft Office Outlook 117

Configurazione dell'elaborazione della posta spam in Microsoft Outlook Express (Windows Mail) 118

RIPRISTINO DELLE IMPOSTAZIONI PREDEFINITE DI ANTI-SPAM

Quando si configura Anti-Spam, è sempre possibile ripristinarne le impostazioni consigliate. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Esse sono raggruppate nel livello di protezione **Consigliato**.

Per ripristinare le impostazioni predefinite di Anti-Spam, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Anti-Spam**.
4. Nella finestra visualizzata, premere il pulsante **Livello predefinito** nella sezione **Riservatezza**.

STATISTICHE ANTI-SPAM

Le informazioni di carattere generale sulle attività eseguite dal componente vengono salvate in un rapporto speciale che riepiloga i dettagli delle attività eseguite dal componente, raggruppate in schede:

- Nella scheda *Eventi* viene generato un elenco completo degli eventi verificatisi durante l'utilizzo del componente. In questo elenco, vengono visualizzati i risultati dell'addestramento di Anti-Spam, ovvero il fattore, la categoria e i motivi delle diverse classificazioni dei messaggi di posta elettronica.

Il menu di scelta rapida consente di eseguire l'addestramento durante la visualizzazione del rapporto. A tale scopo, selezionare il nome del messaggio, aprire il menu di scelta rapida cliccando con il pulsante destro del mouse, quindi selezionare **Contrassegna come spam**, se il messaggio è spam oppure **Contrassegna come non spam** se il messaggio selezionato è valido. Inoltre, in base alle informazioni ottenute dall'analisi del messaggio, è possibile ingrandire gli elenchi di elementi consentiti e bloccati di Anti-Spam. A tal fine, utilizzare le voci corrispondenti sul menu di scelta rapida.

- Nella scheda *Impostazioni* sono disponibili le impostazioni per il filtraggio della posta elettronica e ulteriori elaborazioni.

Per visualizzare informazioni sulle attività del componente, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Rapporto** dal menu di scelta rapida del componente **Anti-Spam**.

CONTROLLO ACCESSI

Controllo Accessi è un nuovo componente di Kaspersky Anti-Virus che consente di controllare l'accesso degli utenti ai dispositivi installati con il componente Controllo dispositivo. Il componente permette di bloccare i tentativi delle applicazioni di accedere a determinati tipi di dispositivi esterni.

Dopo averlo installato, Controllo dispositivo viene disabilitato.

➧ *Per abilitare Controllo dispositivo, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Controllo dispositivo**.
3. Nella parte destra della finestra, selezionare la casella ☑ **Abilita Controllo dispositivo**.

➧ *Per modificare le impostazioni di Controllo dispositivo, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Controllo dispositivo**.
4. Nella finestra visualizzata, apportare le modifiche desiderate alle impostazioni del componente.

IN QUESTA SEZIONE

Controllo dispositivo. Limitazione dell'utilizzo di dispositivi esterni 122

Controllo dispositivo. Disabilita autorun 123

Statistiche di Controllo Accessi 123

CONTROLLO DISPOSITIVO. LIMITAZIONE DELL'UTILIZZO DI DISPOSITIVI ESTERNI

Il modulo Controllo dispositivo consente di controllare le interazioni tra le applicazioni e i dispositivi esterni installati sul computer.

Per impostazione predefinita, Controllo dispositivo consente di accedere a qualsiasi dispositivo.

➧ *Per limitare l'accesso delle applicazioni ai dispositivi, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Controllo dispositivo**.
4. Nella finestra visualizzata, cliccare sul pulsante **Impostazioni**.
5. Nella finestra **Impostazioni: Controllo dispositivo** visualizzata, selezionare le caselle ☑ per i tipi di dispositivi che si desidera bloccare.

Per convalidare le modifiche, è necessario ricollegare il dispositivo (nel caso di dispositivi Firewire o USB) o riavviare il computer (per altri tipi di dispositivi).

CONTROLLO DISPOSITIVO. DISABILITA AUTORUN

È possibile bloccare l'autorun mediante le opzioni seguenti:

- Blocca esecuzione automatica per tutti i dispositivi, che consente di disabilitare la funzione Esecuzione automatica / AutoPlay implementata in Microsoft Windows. Tale funzionalità permette di leggere i dati e di eseguire automaticamente i programmi da un supporto rimovibile connesso al computer.
- Blocca esecuzione di autorun.inf, che consente di bloccare i tentativi non autorizzati delle applicazioni in esecuzione da supporti rimovibili. Tale opzione permette di bloccare eventuali tentativi del sistema operativo di eseguire istruzioni potenzialmente pericolose nel file autorun.inf, senza disabilitare completamente la funzionalità AutoPlay.

Per impostazione predefinita, l'autorun è bloccato. Poiché gli hacker utilizzano spesso l'opzione autorun per diffondere virus mediante unità rimovibili, Kaspersky Lab consiglia di bloccare questa funzionalità.

Per bloccare l'autorun, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Impostazioni** dal menu di scelta rapida del componente **Controllo dispositivo**.
4. Nella finestra visualizzata, cliccare sul pulsante **Impostazioni**.
5. Nella finestra **Impostazioni: Controllo dispositivo** dispositivo visualizzata, sezione **Autorun**, selezionare ☑ le caselle corrispondenti.

Per convalidare le modifiche, riavviare il computer.

STATISTICHE DI CONTROLLO ACCESSI

Tutte le operazioni eseguite da Controllo dispositivo vengono registrate in un rapporto speciale che riepiloga i dettagli delle operazioni eseguite dal componente, raggruppate nelle schede seguenti:

- Nella scheda *Periferiche*, vengono elencati tutti i dispositivi esterni bloccati dal modulo.
- Nella scheda *Impostazioni* vengono visualizzate le impostazioni che controllano il funzionamento di Controllo Accessi.

Per visualizzare informazioni sulle attività del componente, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la voce **Rapporto** dal menu di scelta rapida del componente **Controllo Accessi**.

SCANSIONE ANTI-VIRUS DEL COMPUTER

Scansione virus è uno degli strumenti più importanti per la protezione del computer. Kaspersky Anti-Virus 6.0 per Windows Workstations MP4 è in grado di eseguire la scansione anti-virus di elementi separati (file, cartelle, dischi, supporti rimovibili) oppure dell'intero computer.

Kaspersky Anti-Virus 6.0 per Windows Workstations MP4 è dotato delle seguenti funzioni di scansione anti-virus:

Scansione

Esame degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi oggetto nel file system del computer.

Scansione completa

Scansione approfondita dell'intero sistema. Gli oggetti seguenti vengono esaminati per impostazione predefinita: memoria di sistema, programmi caricati all'avvio, backup di sistema, database di posta, dischi rigidi, unità rimovibili e unità di rete.

Scansione rapida

Scansione anti-virus degli oggetti di avvio del sistema operativo.

Per impostazione predefinita, le seguenti attività vengono eseguite con le impostazioni consigliate. È possibile modificare tali impostazioni e pianificare l'esecuzione delle attività.

Inoltre, è possibile esaminare qualsiasi oggetto (ad esempio un'unità disco rigido su cui sono archiviati programmi software e giochi, database di posta elettronica trasferiti dall'ufficio, file compressi ricevuti tramite posta elettronica e così via) senza creare un'attività di scansione specifica. È possibile selezionare un oggetto da esaminare mediante l'interfaccia di Kaspersky Anti-Virus o gli strumenti standard di Microsoft Windows (ad esempio **Esplora risorse**, **Desktop** ecc.). Posizionare il cursore sul nome dell'oggetto desiderato, cliccare con il pulsante destro del mouse per aprire il menu di scelta rapida di Microsoft Windows e scegliere l'opzione **Scansione Anti-Virus**.

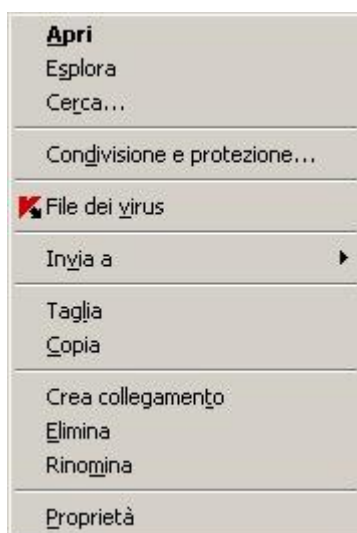



Fig. 7. Menu di scelta rapida di Microsoft Windows

In seguito a una scansione, inoltre, è possibile visualizzarne il rapporto, che contiene informazioni complete sugli eventi verificatisi durante l'esecuzione delle attività.

➡ *Per modificare le impostazioni delle attività di scansione anti-virus, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, apportare le modifiche necessarie nelle impostazioni dell'attività selezionata.

Per passare al rapporto della scansione anti-virus, eseguire le seguenti operazioni:

1. Aprire la finestra principaledell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Cliccare sul pulsante **Rapporto**.

IN QUESTA SEZIONE

Avvio della scansione anti-virus 125
Creazione di un elenco di oggetti da esaminare 126
Modifica del livello di protezione 127
Modifica delle azioni da eseguire sugli oggetti rilevati 127
Modifica del tipo di oggetti da esaminare 129
Ottimizzazione della scansione 129
Scansione dei file compositi 130
Tecnologia di scansione 130
Modifica del metodo di scansione 131
Prestazioni del computer durante l'esecuzione delle attività 131
Modalità di esecuzione: specifica di un account 132
Modalità di esecuzione: creazione di una pianificazione 132
Funzioni dell'avvio pianificato delle attività 133
Statistiche della scansione anti-virus 133
Assegnazione delle impostazioni di scansione comuni per tutte le attività 134
Ripristino delle impostazioni di scansione predefinite 134

AVVIO DELLA SCANSIONE ANTI-VIRUS

È possibile avviare un'attività di scansione anti-virus con una delle due modalità seguenti:

- dal menu di scelta rapida di Kaspersky Anti-Virus;
- dalla finestra principale di Kaspersky Anti-Virus.

Le informazioni sull'esecuzione dell'attività verranno visualizzate nella finestra principale di Kaspersky Anti-Virus.

È inoltre possibile selezionare l'oggetto da esaminare utilizzando gli strumenti standard del sistema operativo Microsoft Windows, ad esempio dalla finestra di **Esplora risorse**, dal **Desktop** e così via.

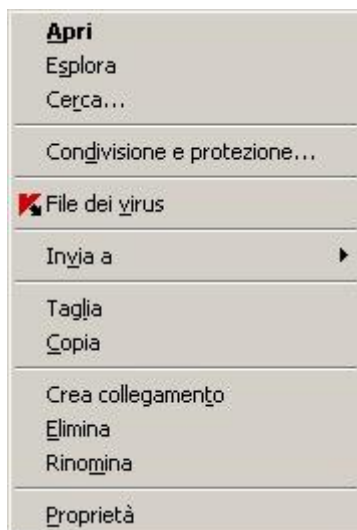



Fig. 8. Menu di scelta rapida di Microsoft Windows

Per avviare un'attività di scansione anti-virus dal menu di scelta rapida, eseguire le seguenti operazioni:

1. Cliccare con il pulsante destro del mouse sull'icona nell'area di notifica della barra delle applicazioni.
2. Selezionare la voce **Scansione** dal menu a discesa. Nella finestra principale dell'applicazione visualizzata, selezionare l'attività **Scansione** (**Scansione completa**, **Scansione rapida**) necessaria. Se necessario, configurare l'attività selezionata e cliccare sul pulsante **Avvia scansione**.
3. In alternativa, è possibile selezionare la voce **Scansione completa** dal menu di scelta rapida. Verrà avviata una scansione completa del computer. L'avanzamento dell'attività verrà visualizzato nella finestra principale di Kaspersky Anti-Virus.

Per avviare l'attività di scansione anti-virus dalla finestra principale dell'applicazione:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Premere il pulsante **Avvia scansione** per la sezione selezionata. Lo stato di avanzamento dell'attività verrà visualizzato nella finestra principale dell'applicazione.

Per avviare una scansione anti-virus di un oggetto selezionato dal menu di scelta rapida di Windows:

1. Cliccare con il pulsante destro del mouse sul nome dell'oggetto selezionato.
2. Selezionare la voce **Scansione Anti-Virus** nel menu di scelta rapida visualizzato. L'avanzamento e i risultati dell'esecuzione dell'attività verranno visualizzati nella finestra delle statistiche.

CREAZIONE DI UN ELENCO DI OGGETTI DA ESAMINARE

Ogni scansione anti-virus comprende il relativo elenco predefinito di oggetti. Per visualizzare un elenco di oggetti, selezionare il nome dell'attività (ad esempio **Scansione completa**) nella sezione **Scansione** della finestra principale dell'applicazione. L'elenco di oggetti verrà visualizzato nella parte destra della finestra.

Gli elenchi degli oggetti da esaminare sono già generati per le attività predefinite create durante l'installazione dell'applicazione.

Per agevolare l'utente, è possibile aggiungere categorie all'ambito della scansione, ad esempio caselle di posta, RAM, oggetti di avvio, backup del sistema operativo e file della cartella Quarantena di Kaspersky Anti-Virus.

Inoltre, quando si aggiunge una cartella che contiene oggetti incorporati nell'ambito della scansione, è possibile modificare la ricorsività. A tale scopo, selezionare l'oggetto desiderato dall'elenco di oggetti da esaminare, aprire il menu di scelta rapida e utilizzare l'opzione **Includi sottocartelle**.

Per creare un elenco di oggetti da esaminare, eseguire le seguenti operazioni:

1. Aprire l'area principaledell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Fare clic sul collegamento **Aggiungi** per la sezione selezionata.
4. Nella finestra **Selezionare oggetto da analizzare** visualizzata, selezionare un oggetto e cliccare sul pulsante **Aggiungi**. Premere il pulsante **OK** dopo aver aggiunto tutti gli oggetti necessari. Per escludere un oggetto dall'elenco di oggetti da esaminare, deselezionare la relativa casella. Per rimuovere un oggetto dall'elenco, selezionarlo e cliccare sul collegamento **Elimina**.

MODIFICA DEL LIVELLO DI PROTEZIONE

Il livello di protezione è una raccolta preimpostata delle impostazioni della scansione. Gli specialisti di Kaspersky Lab distinguono tre livelli di protezione. La decisione sul livello da selezionare si basa sulle preferenze personali:

- Se si sospetta che la possibilità che il computer venga infettato sia alta, selezionare un livello di protezione alto.
- Si tratta del livello più appropriato nella maggior parte dei casi e in genere consigliato dagli specialisti Kaspersky Lab.
- Se si utilizzano applicazioni che richiedono quantità notevoli di risorse RAM, selezionare il livello di protezione basso in quanto in questa modalità l'applicazione impiega una quantità inferiore di risorse di sistema.

Se nessuno dei livelli preimpostati risulta soddisfacente, è possibile configurare la scansione manualmente. Di conseguenza, il nome del livello di protezione cambierà in **Personalizzato**. Per ripristinare le impostazioni predefinite di scansione, selezionare uno dei livelli di protezione preimpostati. Per impostazione predefinita, il livello di scansione impostato è **Consigliato**.

Per modificare il livello di protezione definito, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, regolare il dispositivo di scorrimento sulla scala. La regolazione del livello di protezione consente di definire la velocità di scansione e il numero totale di file esaminato: minore è il numero di file sottoposti a scansione anti-virus, maggiore sarà la velocità di scansione. È inoltre possibile cliccare sul pulsante **Personalizza** e modificare le impostazioni nella finestra visualizzata secondo necessità. Il livello di protezione verrà modificato in **Personalizzato**.

MODIFICA DELLE AZIONI DA ESEGUIRE SUGLI OGGETTI RILEVATI

Se in seguito a una scansione anti-virus viene rilevato un oggetto infetto o potenzialmente tale, l'elaborazione successiva dell'applicazione varia in base allo stato dell'oggetto e all'azione selezionata.

In base ai risultati della scansione, è possibile che a un oggetto venga assegnato uno dei seguenti stati:

- stato programma dannoso (ad esempio *virus*, *Trojan*);
- stato *potenzialmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Il dubbio sorge quando l'applicazione rileva nel file una sequenza di codice di un virus sconosciuto o il codice modificato di un virus conosciuto.

Per impostazione predefinita, tutti i file infetti sono sottoposti a disinfezione e tutti quelli potenzialmente infetti vengono messi in quarantena.

SE L'AZIONE SCELTA È	SE VIENE RILEVATO UN OGGETTO PERICOLOSO O POTENZIALMENTE INFETTO
Richiedi intervento utente al termine della scansione	L'applicazione rimanda l'elaborazione degli oggetti fino al termine della scansione. Quando la scansione è stata completata, viene visualizzata la finestra delle statistiche con un elenco degli oggetti rilevati e viene chiesto se si desidera elaborare gli oggetti.
Richiedi intervento utente durante la scansione	Verrà visualizzato un messaggio di avviso con le informazioni sul codice dannoso che ha infettato o potenzialmente infettato l'oggetto e con diverse opzioni di opzioni supplementari.
Non richiedere intervento utente	L'applicazione crea un rapporto con le informazioni relative agli oggetti rilevati senza elaborarli o segnalarli all'utente. Questa modalità dell'applicazione non è consigliata, in quanto lascia gli oggetti infetti o potenzialmente infetti nel computer, rendendo pressoché inevitabile la diffusione dell'infezione.
Non richiedere intervento utente ☑ **Disinfetta**	L'applicazione tenta di disinfettare l'oggetto senza richiedere una conferma dall'utente. Se il tentativo di disinfezione dell'oggetto non riesce, quest'ultimo verrà bloccato (se non è possibile disinfettare l'oggetto) oppure gli verrà assegnato lo stato di *potenzialmente infetto* (se l'oggetto è considerato sospetto) e verrà messo in Quarantena. Le informazioni rilevanti vengono registrate nel rapporto. In un secondo momento sarà possibile provare a disinfettare l'oggetto.
Non richiedere intervento utente ☑ **Disinfetta** ☑ **Elimina se la disinfezione non riesce**	L'applicazione tenta di disinfettare l'oggetto senza richiedere una conferma dall'utente. Se la disinfezione non riesce, l'oggetto viene eliminato.
Non richiedere intervento utente ☐ **Disinfetta** ☑ **Elimina**	L'applicazione elimina automaticamente l'oggetto.

Prima di provare a disinfettare o eliminare un oggetto infetto, Kaspersky Anti-Virus ne crea una copia di backup e la archivia nel Backup per consentirne il ripristino o la disinfezione in un secondo momento.

Per modificare l'azione da eseguire sugli oggetti rilevati, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella sezione **Azione**, immettere le modifiche desiderate nella finestra visualizzata.

MODIFICA DEL TIPO DI OGGETTI DA ESAMINARE

Quando si specificano i tipi di oggetti da esaminare, vengono definiti il formato e le dimensioni dei file su cui verrà eseguita l'attività di scansione anti-virus selezionata.

Quando si selezionano i tipi di file, si tenga presente quanto segue:

- Alcuni formati di file (ad esempio *.txt*) presentano un rischio alquanto basso di contenere codice dannoso attivabile. Altri formati, al contrario, contengono o possono contenere codice eseguibile (*exe*, *dll*, *doc).* Il rischio di penetrazione ed attivazione di codice nocivo in tali file è piuttosto alto.
- È importante ricordare che un utente malintenzionato può inviare un virus al computer in un file con estensione *txt* che in realtà è un file eseguibile rinominato come *txt*. Selezionando l'opzione **Scansione file per estensione**, tale file viene ignorato dalla scansione. Se è stata selezionata l'opzione **Scansione file per formato**, indipendentemente dall'estensione, la protezione del file analizza l'intestazione del file e può determinare se si tratta di un file .exe. Tale file sarà sottoposto ad una scansione anti-virus approfondita.

Per modificare il tipo di oggetto esaminato:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Ambito**, sezione **Tipi di file**, selezionare le impostazioni necessarie.

OTTIMIZZAZIONE DELLA SCANSIONE

È possibile ridurre il tempo di scansione e velocizzare Kaspersky Anti-Virus. Per ottenere questo risultato, è necessario eseguire la scansione solo dei file nuovi e dei file stati modificati dopo l'ultima scansione. Questa modalità si applica sia ai file semplici che composti.

Inoltre, è possibile imporre una limitazione alla lunghezza di scansione. Una volta trascorso l'intervallo di tempo specificato, la scansione del file viene interrotta. È inoltre possibile limitare la dimensione del file da esaminare. Il file verrà ignorato in caso di dimensione superiore al valore impostato.

Per esaminare soltanto i file nuovi e modificati, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Ambito**, nella sezione **Ottimizzazione della scansione**, selezionare la casella **Esamina solo file nuovi e modificati**.

Per imporre una restrizione temporale alla durata della scansione:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.

4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.

5. Nella finestra visualizzata, sulla scheda **Ambito**, nella sezione **Ottimizzazione della scansione**, selezionare la casella ☑ **Esamina solo file nuovi e modificati** e specificare la durata della scansione nel campo corrispondente.

➧ *Per limitare la dimensione del file da esaminare, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).

3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.

4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.

5. Nella finestra visualizzata, scheda **Ambito**, cliccare sul pulsante **Avanzate**.

6. Nella finestra **File compositi** visualizzata, selezionare la casella ☑ **Non decomprimere i file compositi di grandi dimensioni** e specificare la dimensione di file nel campo adiacente.

SCANSIONE DEI FILE COMPOSITI

Un metodo comune per nascondere i virus consiste nell'incorporarli in file compositi: archivi, database e così via. Per rilevare i virus nascosti in questo modo, è necessario decomprimere un file composito e questa operazione può ridurre significativamente la velocità di scansione.

Per ogni tipo di file composito, è possibile scegliere di analizzare tutti i file oppure solo quelli nuovi. Per farlo, utilizzare il collegamento accanto al nome dell'oggetto. Il relativo valore verrà modificato quando si clicca con il pulsante sinistro del mouse su di esso. Se si seleziona la modalità di scansione dei soli file nuovi e modificati, non sarà possibile selezionare il tipo di file compositi da sottoporre a scansione.

➧ *Per modificare l'elenco dei file compositi esaminati:*

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).

3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.

4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.

5. Nella finestra visualizzata, sulla scheda **Ambito**, sezione **Scansione dei file compositi**, selezionare il tipo di file compositi richiesto da esaminare.

TECNOLOGIA DI SCANSIONE

È inoltre possibile specificare la tecnologia da utilizzare durante la scansione:

- **iChecker**. Questa tecnologia è in grado di aumentare la velocità di scansione escludendo determinati oggetti dalla scansione. Un oggetto viene escluso dalla scansione utilizzando uno speciale algoritmo che prende in considerazione la data di rilascio dei database del programma, la data dell'ultima scansione dell'oggetto e le modifiche alle impostazioni di scansione.

  Ad esempio, si dispone di un file di archivio esaminato da Kaspersky Anti-Virus a cui è stato assegnato lo stato *non infetto*. Alla scansione successiva, l'applicazione ignorerà questo archivio, a meno che non sia stato modificato o non siano state modificate le impostazioni di scansione. Se la struttura dell'archivio risulta modificata mediante aggiunta di un nuovo oggetto, oppure se le impostazioni di scansione sono state modificate o i database dell'applicazione aggiornati, il programma esaminerà nuovamente l'archivio.

iChecker presenta tuttavia delle limitazioni: non risulta efficace con file di grandi dimensioni e si applica solo ad oggetti con una struttura riconoscibile dall'applicazione, ad esempio file di tipo exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar.

- **iSwift**. Questa tecnologia è stata sviluppata a partire dalla tecnologia iChecker per i computer che utilizzano un file system di tipo NTFS. Anche iSwift presenta delle limitazioni: è associata a un percorso di file specifico nel file system e può essere applicata solo ad oggetti in NTFS.

Per utilizzare la tecnologia di scansione degli oggetti, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Avanzate**, sezione **Tecnologie di scansione**, abilitare la tecnologia desiderata.

MODIFICA DEL METODO DI SCANSIONE

È possibile utilizzare l'*analisi euristica* come metodo di scansione, che analizza le azioni eseguite da un oggetto sul sistema. Se tali azioni sono tipiche di oggetti dannosi, è probabile che l'oggetto venga classificato come dannoso o sospetto.

È inoltre possibile impostare il livello di dettaglio per l'analisi euristica spostando il cursore in una delle seguenti posizioni: **Superficiale**, **Medio** o **Approfondito**.

Oltre a questo metodo, è possibile utilizzare la scansione Rootkit. Il *rootkit* è una serie di strumenti in grado di nascondere applicazioni dannose nel sistema operativo. Queste utilità vengono inserite nel sistema, nascondendo la loro presenza e quella dei processi, delle cartelle e delle chiavi di registro di altri programmi dannosi installati con il rootkit. Se la scansione è abilitata, è possibile specificare il livello di dettaglio (analisi avanzata) per rilevare i rootkit, che esegue una scansione accurata di tali programmi attraverso l'analisi di un gran numero di oggetti di vario tipo.

Per specificare il metodo di scansione da utilizzare:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Avanzate**, sezione **Metodi di scansione**, selezionare le tecnologie di scansione desiderate.

PRESTAZIONI DEL COMPUTER DURANTE L'ESECUZIONE DELLE ATTIVITÀ

È possibile posticipare le attività di scansione anti-virus per limitare il carico sulla CPU (Central Processing Unit) e sui sottosistemi di archiviazione su disco.

L'esecuzione di attività di scansione aumenta il carico sulla CPU e sui sottosistemi del disco, con conseguente rallentamento dell'esecuzione delle altre applicazioni. In questi casi, per impostazione predefinita Kaspersky Anti-Virus sospende l'esecuzione delle attività anti-virus e libera le risorse di sistema per le applicazioni dell'utente.

Alcune applicazioni, tuttavia, verranno avviate immediatamente dopo il rilascio delle risorse della CPU e verranno eseguite in background. Per fare in modo che la scansione non dipenda dalle prestazioni di tali applicazioni, è consigliabile evitare di assegnare loro risorse del sistema.

Si noti che questa impostazione può essere configurata singolarmente per ciascuna attività di scansione anti-virus. In questo caso, la configurazione di un'attività specifica ha una priorità più alta.

Per posticipare l'esecuzione delle attività di scansione anti-virus quando rallentano altre applicazioni, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di protezione**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Avanzate**, sezione **Metodi di scansione**, selezionare la casella **Concedi risorse ad altre applicazioni**.

MODALITÀ DI ESECUZIONE: SPECIFICA DI UN ACCOUNT

È possibile specificare un account utilizzato dall'applicazione durante l'esecuzione di una scansione anti-virus.

Per avviare l'attività con i privilegi di un altro account utente:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Livello di sicurezza**, fare clic sul pulsante **Personalizza**.
5. Nella finestra visualizzata, sulla scheda **Modalità esecuzione**, sezione **Utente**, selezionare la casella **Esegui l'attività come**. Specificare il nome utente e la password.

MODALITÀ DI ESECUZIONE: CREAZIONE DI UNA PIANIFICAZIONE

Tutte le attività di scansione anti-virus possono essere avviate manualmente o in base a una pianificazione.

L'impostazione di pianificazione predefinita per le attività create durante l'installazione del programma è disattivata. L'eccezione è l'attività di scansione rapida, che viene avviata a ogni avvio del computer.

Quando si crea una pianificazione all'avvio delle attività, è necessario impostare l'intervallo delle scansioni.

Se per qualsiasi motivo non è possibile avviare l'attività, ad esempio perché all'ora prevista il computer era spento, è possibile configurare l'attività in modo che venga avviata automaticamente non appena possibile.

Per modificare una pianificazione per le attività di scansione:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).

3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, premere il pulsante **Cambia** nella sezione **Modalità esecuzione**.
5. Apportare le modifiche necessarie nella finestra **Pianifica** visualizzata.

Per configurare l'avvio automatico delle attività ignorate:

1. Aprire la finestra principaledell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, premere il pulsante **Cambia** nella sezione **Modalità esecuzione**.
5. Nella finestra **Pianifica** visualizzata, sezione **Impostazioni di pianificazione**, selezionare la casella ☑ **Esegui attività se saltata**.

FUNZIONI DELL'AVVIO PIANIFICATO DELLE ATTIVITÀ

Tutte le attività di scansione anti-virus possono essere avviate manualmente o in base a una pianificazione.

Le attività pianificate includono funzionalità aggiuntive, ad esempio è possibile selezionare la casella *Sospendi la scansione pianificata se lo screensaver non è attivo o il computer non è bloccato*. Questa funzionalità consente di rimandare l'avvio dell'attività finché l'utente non avrà terminato di lavorare al computer. Pertanto, l'attività di scansione non richiederà l'utilizzo delle risorse del sistema durante le ore lavorative.

Per avviare le attività di scansione solo quando il computer non è più in uso, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione completa, Scansione rapida**.
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, sezione **Modalità esecuzione**, selezionare la casella ☑ **Sospendi la scansione se lo screensaver non è attivo e il computer non è bloccato**.

STATISTICHE DELLA SCANSIONE ANTI-VIRUS

Le informazioni generali su ciascuna attività di scansione anti-virus sono disponibili nella finestra delle statistiche, in cui è possibile verificare la quantità di oggetti sottoposti a scansione nonché la quantità di oggetti pericolosi e sospetti soggetti a elaborazione. Questa finestra, inoltre, consente di trovare informazioni sull'ora di avvio e di completamento dell'ultima attività di scansione eseguita e sulla durata della scansione.

Le informazioni generali sui risultati della scansione vengono raggruppati nelle schede seguenti:

- Nella scheda *Rilevati* vengono elencati tutti gli oggetti pericolosi rilevati durante l'esecuzione di un'attività.
- Nella scheda *Eventi* vengono elencati tutti gli eventi verificatisi durante l'esecuzione di un'attività.
- Nella scheda *Statistiche* sono disponibili dati statistici sugli oggetti esaminati.
- Nella scheda *Impostazioni* sono disponibili le impostazioni, che determinano le modalità di esecuzione di un'attività.

Se durante la scansione si sono verificati errori, provare a eseguirla di nuovo. Se in seguito a questo tentativo viene restituito un errore, si consiglia di salvare il rapporto sui risultati dell'attività in un file mediante il pulsante **Salva con nome**. Quindi, contattare il Servizio di supporto tecnico e inviare il file di rapporto. Gli specialisti di Kaspersky Lab saranno in grado di offrire assistenza appropriata.

Per visualizzare le statistiche di un'attività di scansione anti-virus, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**), creare un'attività di scansione e avviarla. Lo stato di avanzamento dell'attività verrà visualizzato nella finestra principale. Cliccare sul collegamento **Dettagli** per passare alla finestra delle statistiche.

ASSEGNAZIONE DELLE IMPOSTAZIONI DI SCANSIONE COMUNI PER TUTTE LE ATTIVITÀ

Ciascuna attività di scansione viene eseguita in base alle impostazioni a essa associate. Per impostazione predefinita, le attività create al momento dell'installazione dell'applicazione vengono eseguite con le impostazioni consigliate dagli esperti di Kaspersky Lab.

È possibile configurare impostazioni di scansione globali per tutte le attività. Verrà utilizzato un set di proprietà per eseguire la scansione anti-virus di un singolo oggetto come punto iniziale.

Per assegnare impostazioni di scansione globali a tutte le attività, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione**.
3. Nella parte destra della finestra visualizzata, sezione **Altre impostazioni attività**, cliccare sul pulsante **Applica**. Confermare le impostazioni globali selezionate nella finestra di dialogo a comparsa.

RIPRISTINO DELLE IMPOSTAZIONI DI SCANSIONE PREDEFINITE

Quando si modificano le impostazioni delle attività, è sempre possibile ripristinare quelle consigliate. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Esse sono raggruppate nel livello di protezione **Consigliato**.

Per ripristinare le impostazioni di scansione dei file predefinite, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Per la sezione selezionata, cliccare sul collegamento con il livello di protezione preimpostato.
4. Nella finestra visualizzata, premere il pulsante **Livello predefinito** nella sezione **Livello di sicurezza**.

AGGIORNAMENTO DELL'APPLICAZIONE

Mantenere l'applicazione aggiornata è un requisito fondamentale per garantire l'affidabilità della protezione del computer. Poiché ogni giorno nascono nuovi virus, Trojan e software dannosi, è importante aggiornare regolarmente l'applicazione per proteggere costantemente i dati personali. Le informazioni sulle minacce e i metodi che consentono di neutralizzarle sono memorizzati nei database dell'applicazione. L'aggiornamento tempestivo di tali database diventa quindi un'operazione fondamentale per garantire una protezione affidabile.

L'aggiornamento dell'applicazione viene scaricato e installato sul computer:

- **Database dell'applicazione**

  La protezione delle informazioni è basata su database contenenti le firme delle minacce e gli attacchi di rete, nonché i metodi per contrastarli. I componenti di protezione si avvalgono di tali database per cercare oggetti pericolosi sul computer e disinfettarli. I database vengono aggiunti ogni ora con record di nuove minacce e metodi utilizzati per neutralizzarli. È pertanto consigliabile aggiornarli regolarmente.

  Oltre ai database dell'applicazione, vengono aggiornati anche i driver di rete che consentono ai componenti dell'applicazione di intercettare il traffico di rete.

- **Moduli dell'applicazione**

  Oltre ai database dell'applicazione, è inoltre possibile aggiornare i moduli dell'applicazione. I pacchetti di aggiornamento risolvono le vulnerabilità dell'applicazione e aggiungono o migliorano le funzionalità esistenti.

I server di aggiornamento di Kaspersky Lab rappresentano l'origine principale degli aggiornamenti per Kaspersky Anti-Virus.

Per scaricare dai server gli aggiornamenti disponibili è necessario disporre di una connessione Internet. Per impostazione predefinita, le impostazioni di connessione a Internet vengono determinate automaticamente. Se le impostazioni del server proxy non vengono configurate automaticamente, è possibile configurare le impostazioni di connessione manualmente.

Durante un aggiornamento, i moduli e i database dell'applicazione nel computer vengono confrontati con quelli dell'origine degli aggiornamenti. Se il computer dispone dell'ultima versione dei database e dei moduli dell'applicazione, viene visualizzata una finestra di notifica che conferma che la protezione del computer è aggiornata. Se i database e i moduli sul computer e sul server di aggiornamento sono diversi, l'applicazione scarica solo la parte incrementale degli aggiornamenti. Il fatto che non vengano scaricati tutti i database e i moduli determina un aumento significativo della velocità di copia dei file e una riduzione del traffico Internet.

Prima di aggiornare i database, in Kaspersky Anti-Virus vengono create copie di backup di questi, affinché sia possibile riutilizzarli in futuro.

Potrebbe essere necessario utilizzare l'opzione di rollback se, ad esempio, i database vengono danneggiati durante il processo di aggiornamento. È possibile eseguire facilmente il rollback alla versione precedente e cercare di aggiornare nuovamente i database.

È possibile copiare gli aggiornamenti recuperati in un'origine locale durante l'aggiornamento dell'applicazione. Tale servizio consente di aggiornare i database e i moduli dell'applicazione sui computer in rete per non intasare il traffico Internet.

È inoltre possibile configurare l'avvio degli aggiornamenti automatici.

Nella sezione **Aggiornamento** viene visualizzato lo stato corrente dei database dell'applicazione.

È possibile visualizzare il rapporto di aggiornamento, che contiene informazioni complete sugli eventi verificatisi durante l'aggiornamento. Una panoramica sull'attività dei virus è disponibile nel sito Web www.kaspersky.com cliccando sul collegamento relativo all'**analisi dell'attività dei virus**.

Per modificare le impostazioni delle attività di aggiornamento, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, apportare le modifiche necessarie nelle impostazioni dell'attività selezionata.

Per passare al rapporto degli aggiornamenti, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Cliccare sul pulsante **Rapporto**.

IN QUESTA SEZIONE

Avvio dell'aggiornamento 136
Rollback dell'ultimo aggiornamento 137
Origine degli aggiornamenti 137
Impostazioni internazionali 138
Utilizzo di un server proxy 138
Modalità di esecuzione: specifica di un account 139
Modalità di esecuzione: creazione di una pianificazione 139
Modifica della modalità di esecuzione dell'attività di aggiornamento 140
Selezione degli oggetti da aggiornare 141
Aggiornamento da una cartella locale 141
Statistiche di aggiornamento 142
Problemi possibili durante l'aggiornamento 142

AVVIO DELL'AGGIORNAMENTO

È possibile avviare l'aggiornamento dell'applicazione in qualsiasi momento. Gli aggiornamenti vengono scaricati dall'origine degli aggiornamenti selezionata.

È possibile aggiornare Kaspersky Anti-Virus utilizzando uno dei due metodi supportati:

- Dal menu di scelta rapida.
- Dalla finestra principale dell'applicazione.

Le informazioni sull'aggiornamento verranno visualizzate nella finestra principale dell'applicazione.

Si noti che gli aggiornamenti vengono distribuiti su un'origine locale durante il processo di aggiornamento, a condizione che tale servizio sia abilitato.

Per avviare l'aggiornamento di Kaspersky Anti-Virus dal menu di scelta rapida:

1. Nell'area di notifica della barra delle applicazioni cliccare con il pulsante destro del mouse sull'icona dell'applicazione.
2. Selezionare la voce **Aggiornamento** dal menu a discesa.

Per avviare l'aggiornamento di Kaspersky Anti-Virus dalla finestra principale dell'applicazione:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Premere il pulsante **Avvia aggiornamento**. Lo stato di avanzamento dell'attività verrà visualizzato nella finestra principale dell'applicazione.

ROLLBACK DELL'ULTIMO AGGIORNAMENTO

All'inizio del processo di aggiornamento, Kaspersky Anti-Virus crea una copia di backup dei moduli dell'applicazione e dei database correnti. In questo modo, se l'aggiornamento non riesce, il programma può continuare a funzionare utilizzando i database precedenti.

L'opzione di rollback è utile, ad esempio, se una parte dei database è stata danneggiata. I database locali possono essere danneggiati dall'utente o da un programma nocivo. Ciò è possibile solo se l'Auto-Difesa dell'applicazione è disabilitata. È possibile riportare i database allo stato precedente e ritentarne l'aggiornamento in un secondo momento.

Per eseguire il rollback alla versione precedente del database:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Cliccare sul collegamento **Rollback ai database precedenti**.

ORIGINE DEGLI AGGIORNAMENTI

Per *origine degli aggiornamenti* si intende una risorsa contenente gli aggiornamenti per i database e i moduli di applicazione di Kaspersky Anti-Virus.

È possibile utilizzare le seguenti origini di aggiornamento:

- *Server di amministrazione* è un repository di aggiornamento centralizzato presente nel Administration Server di Kaspersky Administration Kit (per ulteriori informazioni consultare il Manuale dell'amministratore per Kaspersky Administration Kit).
- *I server degli aggiornamenti di Kaspersky Lab* sono siti Web speciali che contengono gli aggiornamenti disponibili per i database e i moduli dell'applicazione per tutti i prodotti Kaspersky Lab.
- *I server FTP o HTTP, le cartelle locali o di rete* sono server o cartelle locali che contengono gli aggiornamenti più recenti.

Se non è possibile accedere ai server degli aggiornamenti di Kaspersky Lab, ad esempio in assenza di una connessione a Internet, chiamare l'ufficio centrale di Kaspersky Lab al numero +7 (495) 797-87-00 o +7 (495) 645-79-39 per richiedere informazioni sui partner di Kaspersky Lab che possono fornire aggiornamenti in formato compresso su floppy o dischi ZIP.

È possibile copiare gli aggiornamenti da un disco rimovibile e caricarli su un sito FTP o HTTP oppure salvarli in una cartella locale o di rete.

Quando si richiedono aggiornamenti su supporti rimovibili, specificare se si desidera ricevere anche gli aggiornamenti per i moduli dell'applicazione.

Se si seleziona una risorsa esterna alla LAN come sorgente degli aggiornamenti, è necessario disporre di una connessione a Internet per poter eseguire l'aggiornamento.

Se sono state selezionate più risorse come origini dell'aggiornamento, l'applicazione cerca di connettersi a esse una dopo l'altra a partire da quella che occupa la prima posizione dell'elenco e recupera gli aggiornamenti dalla prima disponibile.

Per scegliere una sorgente degli aggiornamenti:

1. Aprire nella finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, sezione **Impostazioni aggiornamento**, cliccare sul pulsante **Configura**.
5. Nella finestra visualizzata, sulla scheda **Origine aggiornamento**, cliccare sul pulsante **Aggiungi**.
6. Selezionare un sito FTP o HTTP oppure immetterne l'indirizzo IP, il nome simbolico o l'URL nella finestra **Seleziona origine aggiornamento** visualizzata.

IMPOSTAZIONI INTERNAZIONALI

Se si utilizzano i server degli aggiornamenti di Kaspersky Lab come origine degli aggiornamenti, è possibile selezionare la posizione ottimale del server da cui scaricare i file. I server Kaspersky Lab sono dislocati in più paesi. La scelta del server più vicino consente di risparmiare tempo e accelerare il download degli aggiornamenti.

Per scegliere il server più vicino:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, sezione **Impostazioni aggiornamento**, cliccare sul pulsante **Configura**.
5. Nella finestra visualizzata, sulla scheda **Origine aggiornamento**, sezione **Impostazioni internazionali**, selezionare l'opzione **Seleziona dall'elenco**, quindi scegliere il paese più vicino alla propria posizione geografica dall'elenco a discesa.

   Se si seleziona la casella **Autorileva**, le informazioni sulla posizione verranno copiate dal registro del sistema operativo durante l'esecuzione dell'aggiornamento.

UTILIZZO DI UN SERVER PROXY

Se si utilizza un server proxy per connettersi a Internet, è necessario configurarne le impostazioni.

Per configurare il server proxy, eseguire le operazioni seguenti:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, sezione **Impostazioni aggiornamento**, cliccare sul pulsante **Configura**.
5. Nella finestra visualizzata, modificare le impostazioni del server proxy sulla scheda **Impostazioni proxy**.

MODALITÀ DI ESECUZIONE: SPECIFICA DI UN ACCOUNT

Kaspersky Anti-Virus è dotato di una funzione che consente di avviare gli aggiornamenti del programma da un altro profilo. Per impostazione predefinita, il servizio è disabilitato e le attività vengono avviate tramite l'account con il quale si è registrati nel sistema.

Poiché l'applicazione può essere aggiornata da un'origine a cui non è possibile accedere (ad esempio la directory degli aggiornamenti di rete) o di cui non si dispone delle autorizzazioni necessarie per accedere al server proxy, è possibile utilizzare tale funzione per eseguire gli aggiornamenti dell'applicazione mediante le credenziali di accesso di un utente che dispone di tali privilegi.

Si noti che se non si esegue l'attività con i privilegi, l'aggiornamento pianificato verrà eseguito con i privilegi dell'account utente corrente. Se al momento non sono registrati utenti sul computer, l'esecuzione degli aggiornamento con un altro account utente non è stato configurato e gli aggiornamenti eseguiti automaticamente verranno eseguiti con i privilegi di SISTEMA.

Per avviare l'attività con i privilegi di un altro account utente:

1. Aprire la finestra principale dell'applicazione .
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, sezione **Impostazioni aggiornamento**, cliccare sul pulsante **Configura**.
5. Nella finestra visualizzata, sulla scheda **Avanzate**, sezione **Modalità esecuzione**, selezionare la casella **Esegui attività come**. Inserire i dati di accesso del profilo con cui si desidera avviare l'attività, ovvero nome utente e password.

MODALITÀ DI ESECUZIONE: CREAZIONE DI UNA PIANIFICAZIONE

Tutte le attività di scansione anti-virus possono essere avviate manualmente o in base a una pianificazione.

Quando si crea una pianificazione relativa alle attività da avviare, è necessario impostare l'intervallo delle attività di aggiornamento.

Se per qualsiasi motivo non è possibile avviare l'attività, ad esempio perché all'ora prevista il computer era spento, è possibile configurare l'attività in modo che venga avviata automaticamente non appena possibile.

Per modificare una pianificazione per le attività di scansione:

1. Aprire la finestra principale dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, premere il pulsante **Cambia** nella sezione **Modalità esecuzione**.
5. Apportare le modifiche necessarie nella finestra **Pianifica** visualizzata.

Per configurare l'avvio automatico delle attività ignorate:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, premere il pulsante **Cambia** nella sezione **Modalità esecuzione**.
5. Nella finestra **Pianifica** visualizzata, sezione **Impostazioni di pianificazione**, selezionare la casella **Esegui attività se saltata**.

MODIFICA DELLA MODALITÀ DI ESECUZIONE DELL'ATTIVITÀ DI AGGIORNAMENTO

È possibile selezionare la modalità di esecuzione dell'attività di aggiornamento di Kaspersky Anti-Virus mediante la configurazione guidata dell'applicazione (per ulteriori informazioni, consultare la sezione "Configurazione delle impostazioni di aggiornamento" a pagina 30). È possibile modificare la modalità di esecuzione selezionata.

L'attività di aggiornamento può essere avviata tramite una delle seguenti modalità:

- **Automaticamente**. Kaspersky Anti-Virus verifica a intervalli specificati la disponibilità di pacchetti di aggiornamento nell'origine degli aggiornamenti. Se vengono rilevati nuovi aggiornamenti, questi vengono scaricati e installati nel computer. Questa è la modalità predefinita.

  Kaspersky Anti-Virus tenterà di eseguire gli aggiornamenti in base agli intervalli specificati nel pacchetto di aggiornamenti precedente. Tale opzione consente a Kaspersky Lab di regolare la frequenza degli aggiornamenti in caso di attacchi da virus e altre situazioni potenzialmente pericolose. L'applicazione riceverà tempestivamente gli ultimi aggiornamenti per i database, gli attacchi di rete e i moduli software, escludendo la possibilità che il malware penetri nel computer.

- **Programmata** (l'intervallo di tempo cambia in base alle impostazioni). Gli aggiornamenti vengono eseguiti automaticamente in base alla pianificazione.

- **Manualmente**. Se si seleziona questa opzione, gli aggiornamenti verranno eseguiti manualmente. Kaspersky Anti-Virus informerà immediatamente l'utente in caso di aggiornamenti necessari.

Per configurare la pianificazione di avvio dell'attività di aggiornamento:

1. Aprire la finestradell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, selezionare la modalità di avvio dell'attività di aggiornamento nella sezione **Modalità esecuzione**. Se l'opzione relativa all'aggiornamento pianificato è selezionata, creare la pianificazione.

SELEZIONE DEGLI OGGETTI DA AGGIORNARE

Gli oggetti da aggiornare sono i componenti che verranno aggiornati:

- database dell'applicazione;
- driver di rete che consentono ai componenti di protezione di intercettare il traffico di rete;
- database degli attacchi di rete utilizzato da Anti-Hacker;
- moduli dell'applicazione.

I database, i driver di rete e il database degli attacchi di rete sono sempre aggiornati, mentre i moduli dell'applicazione vengono aggiornati esclusivamente se configurati correttamente.

Se è disponibile un set di moduli dell'applicazione nell'origine degli aggiornamenti durante l'aggiornamento, Kaspersky Anti-Virus li scaricherà e installerà al riavvio del computer. Gli aggiornamenti dei moduli scaricati non verranno installati fino al riavvio del computer.

Se il successivo aggiornamento dell'applicazione viene eseguito prima del riavvio del computer e, quindi, prima dell'installazione dei precedenti aggiornamenti per il modulo dell'applicazione, verranno aggiornate solo le firme delle minacce.

➡ *Per scaricare e installare gli aggiornamenti per i moduli dell'applicazione, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, sezione **Impostazioni aggiornamento**, selezionare la casella ☑ **Aggiorna moduli programma**.

AGGIORNAMENTO DA UNA CARTELLA LOCALE

La procedura di recupero degli aggiornamenti da una cartella locale viene organizzata nel modo seguente:

1. Uno dei computer della rete recupera un pacchetto di aggiornamento di Kaspersky Anti-Virus da un server di Kaspersky Lab o da un server mirror che ospita un insieme corrente di aggiornamenti. Gli aggiornamenti recuperati vengono salvati in una cartella condivisa.
2. Gli altri computer della rete accedono alla cartella condivisa per recuperare gli aggiornamenti.

Kaspersky Anti-Virus 6.0 è in grado di recuperare esclusivamente i pacchetti di aggiornamento dai server di Kaspersky Lab. È consigliabile distribuire gli aggiornamenti per le altre applicazioni di Kaspersky Lab tramite il Kaspersky Administration Kit.

➡ *Per abilitare la modalità di aggiornamento, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, cliccare sul pulsante **Configura**.

5. Nella finestra visualizzata, sulla scheda **Avanzate**, sezione **Aggiorna distribuzione**, selezionare la casella **Copia aggiornamenti nella cartella** e nel campo sottostante specificare il percorso della cartella condivisa in cui verranno copiati gli aggiornamenti scaricati. È inoltre possibile selezionare il percorso nella finestra visualizzata cliccando sul pulsante **Sfoglia**.

Se si desidera che gli aggiornamenti dell'applicazione vengano eseguiti dalla cartella condivisa selezionata, eseguire le seguenti operazioni su tutti i computer della rete:

1. Aprire la finestra principaledell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Per la sezione selezionata, cliccare sul collegamento con la modalità di esecuzione preimpostata.
4. Nella finestra visualizzata, cliccare sul pulsante **Configura**.
5. Nella finestra visualizzata, sulla scheda **Origine aggiornamento**, cliccare sul pulsante **Aggiungi**.
6. Nella finestra **Seleziona origine aggiornamento** visualizzata, selezionare la cartella oppure immettere il percorso completo della cartella nel campo **Origine**.
7. Deselezionare la casella **Server degli aggiornamenti Kaspersky Lab** nella scheda **Origine aggiornamento**.

STATISTICHE DI AGGIORNAMENTO

Nella finestra delle statistiche sono disponibili informazioni generali sulle attività di aggiornamento. In questa finestra, è inoltre possibile visualizzare gli eventi verificatisi durante l'esecuzione di un'attività (scheda *Eventi*) e visualizzare l'elenco di impostazioni che determinano l'esecuzione dell'attività (scheda *Impostazioni*).

Se durante la scansione si sono verificati errori, provare a eseguirla di nuovo. Se in seguito a questo tentativo viene restituito un errore, si consiglia di salvare il rapporto sui risultati dell'attività in un file mediante il pulsante **Salva con nome**. Quindi, contattare il Servizio di supporto tecnico e inviare il file di rapporto. Gli specialisti di Kaspersky Lab saranno in grado di offrire assistenza appropriata.

Un breve riepilogo delle statistiche di aggiornamento è disponibile nella parte superiore della finestra delle statistiche. Include la dimensione degli aggiornamenti scaricati e installati, la velocità e la durata dell'aggiornamento, e ulteriori informazioni.

Per visualizzare le statistiche di un'attività di scansione anti-virus, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiorna**, creare un'attività di aggiornamento e avviarla. Lo stato di avanzamento dell'attività verrà visualizzato nella finestra principale. Cliccare sul collegamento **Dettagli** per passare alla finestra delle statistiche.

PROBLEMI POSSIBILI DURANTE L'AGGIORNAMENTO

Quando si aggiornano i moduli dell'applicazione o le firme delle minacce di Kaspersky Anti-Virus, è possibile che si verifichino errori associati a configurazioni di aggiornamento non valide, problemi di connessione ecc. In questa sezione della Guida viene elencata la maggior parte degli errori e vengono indicate le possibili soluzioni per eliminarli. Se si riscontrano errori non descritti nella Guida o si desidera ricevere suggerimenti dettagliati per eliminarli, è possibile trovare ulteriori informazioni nella Knowledge Base disponibile nel portale Web di assistenza tecnica nella sezione "Se un programma ha generato un errore...". Se i suggerimenti descritti in questa sezione non risolvono l'errore o in assenza di informazioni nella Knowledge Base, inviare una richiesta al team di assistenza tecnica.

ERRORI DI CONFIGURAZIONE

Gli errori appartenenti a questa categoria si verificano nella maggior parte dei casi a causa di un'installazione non corretta dell'applicazione oppure a causa di modifiche apportate alla configurazione dell'applicazione, che ha provocato un perdita di funzionalità.

Suggerimenti generali:

Se vengono generati errori di questo tipo, si consiglia di riavviare gli aggiornamenti. Se l'errore persiste, contattare l'assistenza tecnica.

Se il problema è causato da un'installazione non appropriata dell'applicazione, si consiglia di reinstallarla.

Nessuna origine aggiornamenti specificata

Le origini specificate non contengono file di aggiornamento. È possibile che non siano state specificate origini degli aggiornamenti nelle impostazioni di aggiornamento. Verificare che le impostazioni di aggiornamento siano configurate correttamente e riprovare.

Errore nella verifica della licenza

Tale errore viene generato se la chiave di licenza utilizzata dall'applicazione è bloccata e posizionata nell'elenco di licenze bloccate.

Errore nel recupero delle impostazioni di aggiornamento

Errore interno durante il recupero delle impostazioni dell'attività di aggiornamento. Verificare che le impostazioni di aggiornamento siano configurate correttamente e riprovare.

Privilegi insufficienti per aggiornare

In genere, tale errore si verifica quando l'account utente utilizzato per avviare l'aggiornamento non dispone di privilegi di accesso all'origine degli aggiornamenti. Si consiglia di verificare che l'account utente disponga dei privilegi necessari.

Tale errore può essere generato anche quando si tenta di copiare i file di aggiornamento in una cartella che non è possibile creare.

Errore interno

Errore logico interno durante l'attività di aggiornamento. Verificare che le impostazioni di aggiornamento siano configurate correttamente e riprovare.

Errore nella verifica degli aggiornamenti

Tale errore viene generato se i file scaricati dall'origine degli aggiornamenti non superano la verifica interna. Ritentare l'aggiornamento in un secondo momento.

ERRORI CHE SI VERIFICANO QUANDO SI LAVORA CON FILE E CARTELLE

Questo tipo di errori si verifica quando l'account utente utilizzato per eseguire gli aggiornamenti dispone di diritti limitati o di nessun diritto ad accedere all'origine degli aggiornamenti o alla cartella in cui sono ubicati gli aggiornamenti.

Suggerimenti generali:

Se si verificano errori di questo tipo, si consiglia di verificare che l'account utente disponga di diritti di accesso sufficienti a tali file e cartelle.

Impossibile creare cartella

Tale errore viene generato se non è possibile creare una cartella durante la procedura di aggiornamento.

Privilegi insufficienti per eseguire le operazioni con i file

Tale errore verifica se l'account utente utilizzato per eseguire l'aggiornamento non dispone di privilegi sufficienti per eseguire operazioni con i file.

File o cartella non trovati

Tale errore si verifica se un file o una cartella necessario negli aggiornamenti è inesistente. Si consiglia di verificare l'esistenza e la disponibilità del file o della cartella specificati.

Errore nelle operazioni con i file Si tratta di un errore logico interno del modulo di aggiornamento durante l'esecuzione delle operazioni con i file.
ERRORI DI RETE Gli errori che rientrano in questa categoria si verificano in caso di problemi di connessione o quando una connessione di rete non è configurata correttamente. Suggerimenti generali: Se si verificano errori di questo tipo, si consiglia di verificare che il computer sia connesso a Internet, le impostazioni di connessione siano configurate correttamente e l'origine degli aggiornamenti sia disponibile. Quindi, ritentare l'aggiornamento. Se il problema persiste, contattare l'assistenza tecnica.
Errore di rete Si è verificato un errore nel recupero dei file di aggiornamento. Se si riscontra questo errore, verificare la connessione di rete del computer.
Connessione interrotta Tale errore si verifica quando l'origine degli aggiornamenti viene interrotta dal server di aggiornamento per qualsiasi motivo.
Timeout operazione rete Timeout della connessione all'origine degli aggiornamenti. Quando si configurano le impostazioni di aggiornamento del programma, è possibile che sia stato impostato un valore di timeout breve per la connessione all'origine degli aggiornamenti. Se il computer non è in grado di stabilire la connessione con il server o con la cartella di aggiornamento durante il periodo specificato, viene restituito questo errore. In tal caso, si consiglia di verificare che le impostazioni del Programma di aggiornamento siano corrette e che l'origine degli aggiornamenti sia disponibile.
Errore di autorizzazione sul server FTP Tale errore si verifica se le impostazioni di autorizzazione del server FTP utilizzate come origine degli aggiornamenti non sono state immesse correttamente. Accertarsi che le impostazioni del server FTP effettivo consentano all'account utente di scaricare file.
Errore di autorizzazione sul server proxy Tale errore viene generato se le impostazioni di aggiornamento mediante un server proxy indicano erroneamente il nome e la password oppure se l'account utente in cui vengono eseguiti tali aggiornamenti non dispone di privilegi di accesso all'origine degli aggiornamenti. Modificare le impostazioni di autorizzazione e ritentare l'aggiornamento.
Errore nella risoluzione del nome DNS Tale errore viene generato se non si rilevano origini degli aggiornamenti. È possibile che l'indirizzo dell'origine degli aggiornamenti non sia indicato correttamente, le impostazioni di rete non siano valide o che il server DNS non sia disponibile. Si consiglia di verificare le impostazioni di aggiornamento e la disponibilità delle origini degli aggiornamenti, quindi riprovare.
Impossibile stabilire la connessione con l'origine degli aggiornamenti Tale errore si verifica in assenza di connessione con l'origine degli aggiornamenti. Verificare che le impostazioni dell'origine degli aggiornamenti siano configurate correttamente e riprovare.
Impossibile stabilire la connessione con il server proxy Tale errore viene generato se le impostazioni di connessione al server proxy non sono indicate correttamente. Per risolvere il problema, si consiglia di verificare che le impostazioni siano configurate correttamente, il server proxy sia disponibile e la connessione Internet sia disponibile, quindi eseguire di nuovo l'aggiornamento.
Errore nella risoluzione del nome DNS del server proxy Tale errore viene generato se non si rileva il server proxy. Si consiglia di verificare che le impostazioni del server proxy siano valide e che il server DNS sia disponibile.

ERRORI CORRELATI AI DATABASE DANNEGGIATI

Tali errori vengono generati in caso di file danneggiati nell'origine degli aggiornamenti.

Suggerimenti generali:

Se si esegue l'aggiornamento dai server Web di Kaspersky Lab, ritentare l'aggiornamento. Se il problema persiste, contattare l'assistenza tecnica.

Se si esegue l'aggiornamento da un'altra origine, ad esempio una cartella locale, si consiglia di eseguire l'aggiornamento dai server Web di Kaspersky Lab. Se l'errore si verifica di nuovo, contattare l'assistenza tecnica di Kaspersky Lab.

File inesistente nell'origine degli aggiornamenti

Tutti i file scaricati e installati sul computer durante il processo di aggiornamento vengono elencati in un file speciale incluso nell'aggiornamento. Tale errore si verifica in presenza di eventuali file nell'elenco di aggiornamenti non disponibile nell'origine degli aggiornamenti.

Errore nella verifica della firma

È possibile che venga restituito questo errore se la firma elettronica digitale del pacchetto di aggiornamento scaricato è danneggiata o non corrisponde alla firma di Kaspersky Lab.

File di indice danneggiato o mancante

Tale errore viene generato se il file di indice in formato .xml utilizzato dall'aggiornamento non esiste nell'origine degli aggiornamenti oppure è danneggiato.

ERRORI CORRELATI ALL'AGGIORNAMENTO CON IL COMPONENTE ADMINISTRATION SERVER DI KASPERSKY ADMINISTRATION KIT

Tali errori sono generati in caso di problemi di aggiornamento dell'applicazione mediante il componente Administration Server di Kaspersky Administration Kit.

Suggerimenti generali:

Innanzitutto, verificare che Kaspersky Administration Kit e i relativi componenti (Administration Server e Network Agent) siano installati e in esecuzione. Ritentare l'aggiornamento. Se l'aggiornamento non riesce, riavviare Network Agent e Administration Server, quindi ritentare l'aggiornamento. Se il problema persiste, contattare l'assistenza tecnica.

Errore di connessione ad Administration Server

Tale errore viene generato se non è possibile stabilire la connessione con il componente Administration Server di Kaspersky Administration Kit. Si consiglia di verificare che il componente NAgent sia installato e in esecuzione.

Errore di registrazione in NAgent

Se si verifica tale errore, attenersi ai suggerimenti generali per la risoluzione di questo tipo di errore. Se l'errore si verifica di nuovo, inviare il file di rapporto dettagliato per l'aggiornamento e Network Agent sul computer al servizio di assistenza servendosi del modulo online. Descrivere la situazione dettagliatamente.

Impossibile stabilire la connessione. Administration Server è occupato e non è in grado di elaborare la richiesta

In tal caso, è necessario tentare l'aggiornamento in un secondo momento.

Impossibile stabilire la connessione con Administration Server / Main Administration Server / NAgent, errore fisico / errore sconosciuto

Se si riscontrano questo tipo di errori, si consiglia di tentare l'aggiornamento in un secondo momento. Se il problema persiste, contattare l'assistenza tecnica.

Errore nel recupero del file da Administration Server, argomento di trasporto non valido

Se l'errore persiste, contattare l'assistenza tecnica.

Errore nel recupero del file da Administration Server

Se si riscontrano questo tipo di errori, si consiglia di tentare l'aggiornamento in un secondo momento. Se il problema persiste, contattare l'assistenza tecnica.

CODICI VARI Tale categoria comprende gli errori che non è possibile includere nelle categorie precedentemente descritte.
File per l'operazione di rollback mancanti Tale errore si verifica se è stato eseguito un altro tentativo di rollback dopo aver completato il rollback degli aggiornamento senza installare nessun aggiornamento. Non è possibile ripetere la procedura di rollback fino al completamento di un aggiornamento riuscito che ripristini un set di file sottoposti a backup.

CONFIGURAZIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE

La finestra delle impostazioni dell'applicazione consente di accedere rapidamente alle principali impostazioni di Kaspersky Anti-Virus 6.0.

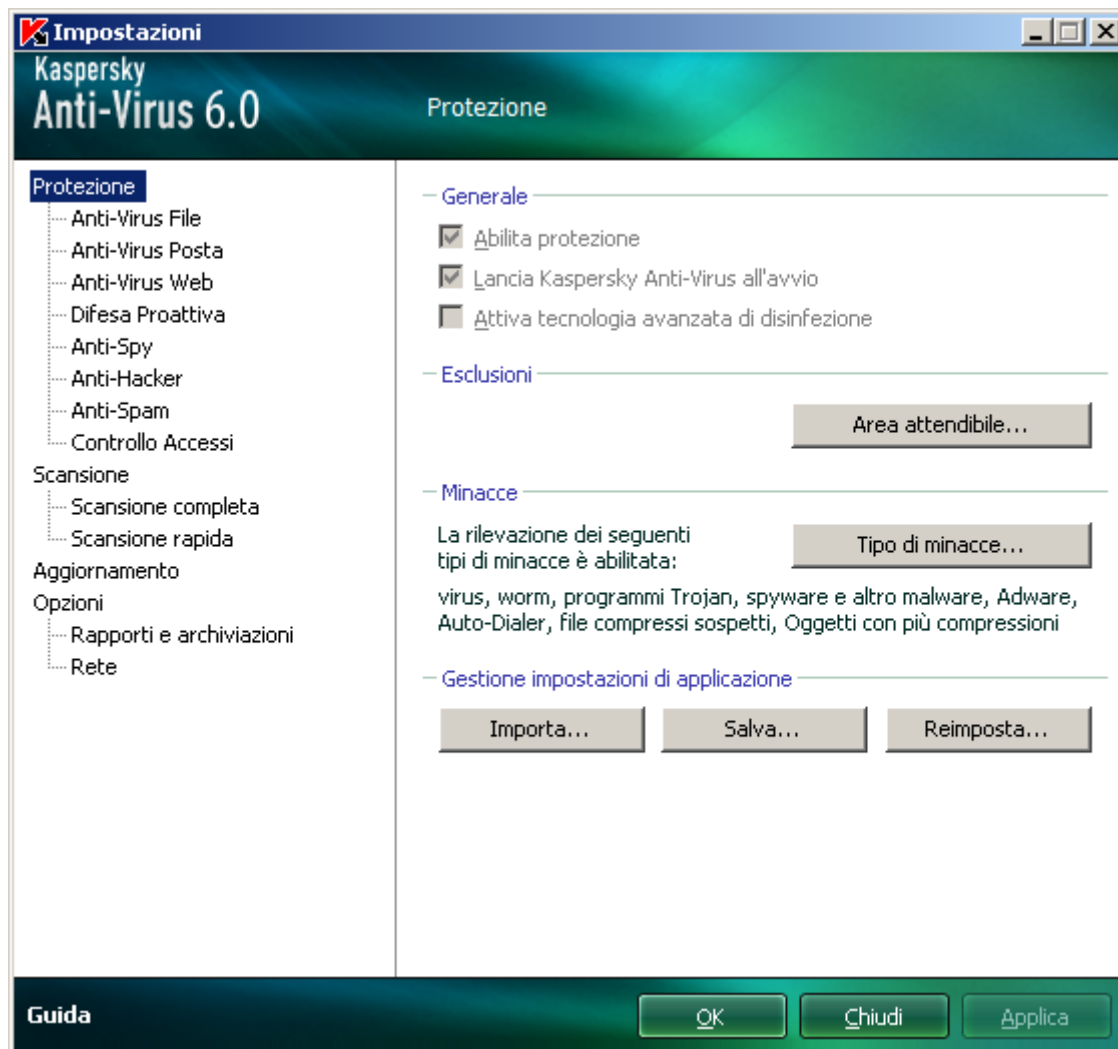



Fig. 9. Finestra di configurazione delle impostazioni dell'applicazione

La finestra è composta da due parti:

- la parte sinistra consente di accedere ai componenti di Kaspersky Anti-Virus, alle attività di scansione anti-virus, alle attività di aggiornamento e così via;
- la parte destra della finestra contiene un elenco di impostazioni relative, ad esempio, al componente e all'attività selezionati nella parte sinistra della finestra.

È possibile aprire questa finestra:

- Dalla finestra principale dell'applicazione. A tale scopo, cliccare sul collegamento **Impostazioni** nella parte superiore della finestra.
- Dal menu di scelta rapida. A tale scopo, selezionare la voce **Impostazioni** dal menu di scelta rapida.

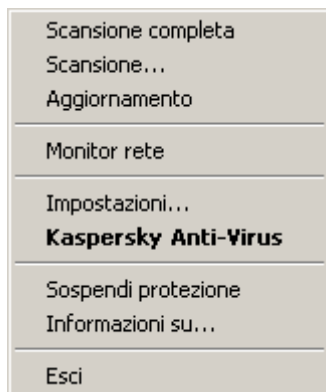



Fig. 10. Menu di scelta rapida

- Dal menu di scelta rapida per componenti singoli. A tale scopo, selezionare la voce **Impostazioni** dal menu.

Fig. 11. Apertura della finestra delle impostazioni dal menu di scelta rapida per un componente singolo

IN QUESTA SEZIONE

Protezione 149

Anti-Virus File 157

Anti-Virus Posta 157

Difesa Proattiva 159

Anti-Spy 159

Anti-Hacker 160

Anti-Spam 161

Scansione 162

Aggiornamento 163

Impostazioni 163

Rapporti e archiviazioni 168

Rete 172

PROTEZIONE

Nella finestra **Protezione** è possibile utilizzare le funzioni avanzate di Kaspersky Anti-Virus elencate di seguito:

- Abilitazione / disabilitazione della protezione dell'applicazione (vedere pagina 150).
- Avvio dell'applicazione all'avvio del sistema operativo (vedere pagina 150).
- Utilizzo della tecnologia avanzata di disinfezione (vedere pagina 150).
- Selezione delle categorie di minacce rilevabili (vedere pagina 151).
- Creazione di un'area attendibile (vedere pagina 151):
  - creazione di una regola di esclusione (vedere pagina 152);
  - specifica di ulteriori impostazioni di esclusione (vedere pagina 153);
  - creazione di un elenco di applicazioni attendibili (vedere pagina 154);
  - esportazione / importazione dei componenti dell'area attendibile (vedere pagina 155).
- Esportazione / importazione delle impostazioni dell'applicazione (vedere pagina 155).
- Ripristino delle impostazioni predefinite dell'applicazione (vedere pagina 156).

ABILITAZIONE / DISABILITAZIONE DELLA PROTEZIONE DEL COMPUTER

Per impostazione predefinita, Kaspersky Anti-Virus viene avviato durante il caricamento del sistema operativo e protegge il computer finché non viene spento. Tutti i componenti di protezione sono in esecuzione.

La protezione offerta dall'applicazione può essere abilitata completamente o parzialmente.

Gli esperti di Kaspersky Lab consigliano di **non disabilitare la protezione**, in quanto questo può portare all'infezione del computer e alla perdita di dati.

Se si disabilita la protezione, tutti i componenti di protezione verranno disabilitati, come indicato da:

- Nomi dei componenti disabilitati inattivi (in grigio) nella finestra principale dell'applicazione.
- Icona dell'applicazione inattiva (in grigio) nell'area di notifica della barra delle applicazioni.
- Colore rosso dell'indicatore di protezione.

In questo caso, la protezione è descritta nel contesto dei componenti di protezione. La disabilitazione dei componenti di protezione non pregiudica l'esecuzione delle attività di scansione anti-virus e degli aggiornamenti di Kaspersky Anti-Virus.

Per disabilitare completamente la protezione:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Deselezionare la casella ☑ **Abilita la protezione**.

AVVIO DELL'APPLICAZIONE ALL'AVVIO DEL SISTEMA OPERATIVO

Se per qualsiasi motivo è necessario arrestare completamente Kaspersky Anti-Virus, selezionare la voce **Esci** dal menu di scelta rapida dell'applicazione. In questo modo, l'applicazione verrà rimossa dalla memoria RAM, causando l'esecuzione del computer in uno stato non protetto.

Per abilitare la protezione del computer, avviare l'applicazione dal menu **Start** → **Tutti i programmi** → **Kaspersky Anti-Virus 6.0** → **Kaspersky Anti-Virus 6.0**.

La protezione può essere anche ripresa automaticamente dopo aver riavviato il sistema operativo.

Per avviare la modalità di avvio dell'applicazione all'avvio del sistema operativo, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la casella ☑ **Lancia Kaspersky Anti-Virus all'avvio**.

UTILIZZO DELLA TECNOLOGIA AVANZATA DI DISINFEZIONE

I programmi dannosi moderni possono invadere i livelli più bassi di un sistema operativo, rendendone praticamente impossibile la rimozione. Kaspersky Anti-Virus chiederà all'utente se desidera eseguite la tecnologia avanzata di disinfezione quando rileva una minaccia attiva nel sistema. In questo modo la minaccia verrà neutralizzata e rimossa dal computer.

Al termine di questa procedura, è necessario riavviare il computer. Dopo aver riavviato il computer, si consiglia di eseguire una scansione anti-virus completa.

Per avviare la procedura avanzata di disinfezione, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Selezionare la casella ☑ **Attiva la tecnologia avanzata di disinfezione**.

SELEZIONE DELLE CATEGORIE DI MINACCE RILEVABILI

Kaspersky Anti-Virus protegge da diversi tipi di programmi pericolosi. A prescindere dalle impostazioni selezionate, viene sempre eseguita la scansione e la disinfezione per eliminare virus e Trojan. Questi programmi infatti possono danneggiare gravemente il computer. Per offrire una maggiore protezione, è possibile ampliare l'elenco di minacce da rilevare, abilitando il controllo di vari programmi potenzialmente pericolosi.

Per selezionare le categorie di minacce rilevabili, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Minacce**, cliccare sul pulsante **Tipi di minacce**.
4. Nella finestra **Tipi di minacce** visualizzata, selezionare le ☑ caselle relative alle categorie di minacce da cui si desidera proteggere il computer.

CREAZIONE DI UN'AREA ATTENDIBILE

L'area attendibile è un elenco di oggetti creati dall'utente non esaminati da Kaspersky Anti-Virus. In altre parole, si tratta di una serie di programmi esclusi dall'ambito di protezione dell'applicazione.

L'utente crea un'area attendibile sulla base delle caratteristiche degli oggetti che utilizza e delle applicazioni installate nel computer. Questo elenco di esclusioni può tornare utile, ad esempio, se Kaspersky Anti-Virus blocca l'accesso a un oggetto o un'applicazione della cui sicurezza l'utente è assolutamente certo.

È possibile escludere dalla scansione determinati formati di file, utilizzare una maschera file oppure escludere un'area specifica (ad esempio una cartella o un'applicazione), processi di programmi oppure oggetti in base alla classificazione dell'Enciclopedia di virus (stato assegnato da Kaspersky Anti-Virus durante una scansione).

Un oggetto di esclusione viene escluso dalla scansione quando il disco o la cartella in cui è ubicato è sottoposto a scansione. Tuttavia, se si seleziona specificamente tale oggetto, la regola di esclusione non verrà applicata a questo.

Per creare un elenco di esclusioni dalla scansione, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Esclusioni**, cliccare sul pulsante **Area attendibile**.
4. Nella finestra visualizzata, configurare le regole di esclusione per gli oggetti (vedere pagina 152) e creare l'elenco di applicazioni attendibili (vedere pagina 154).

VEDERE ANCHE

Creazione di una regola di esclusione 152

Ulteriori impostazioni di esclusione 153

Maschere di esclusione file consentite 153

Maschere di esclusione consentite secondo la Virus Encyclopedia 154

Creazione dell'elenco di applicazioni attendibili 154

Esportazione/importazione di componenti di area attendibile 155

CREAZIONE DI UNA REGOLA DI ESCLUSIONE

Le *regole di esclusione* sono insiemi di condizioni utilizzati da Kaspersky Anti-Virus per verificare se sia possibile evitare la scansione di un oggetto.

È possibile escludere dalla scansione determinati formati di file, utilizzare una maschera file o escludere una determinata area, ad esempio una cartella o un'applicazione, processi di programmi o oggetti in base alla classificazione dell'Enciclopedia di virus.

Il *tipo di minaccia* è lo stato assegnato da Kaspersky Anti-Virus a un oggetto al momento della scansione. Tale stato viene assegnato in base alla classificazione di malware e riskware individuata nell'Enciclopedia di virus di Kaspersky Lab.

Il software potenzialmente pericoloso non svolge una funzione dannosa vera e propria ma può essere utilizzato dagli hacker come componente ausiliario di un codice nocivo in quanto contiene errori e vulnerabilità. Tale categoria comprende, ad esempio, applicazioni di amministrazione remota, client IRC, server FTP, utilità di vario genere per interrompere o nascondere processi, keylogger, macro di password, autodialer e così via. Tali applicazioni software non vengono considerate come virus ma possono essere suddivise in diversi tipi, ad esempio Adware, Joke, Riskware ecc. (per ulteriori informazioni sulle applicazioni software potenzialmente pericolose rilevate da Kaspersky Anti-Virus, consultare l'Enciclopedia di virus disponibile all'indirizzo www.viruslist.com (http://www.viruslist.com/en/viruses/encyclopedia)). Dopo la scansione, questi programmi possono essere bloccati. Poiché molti di questi programmi vengono sfruttati ampiamente dagli utenti, è possibile escluderli dalla scansione. A tale scopo, è necessario aggiungere il nome della minaccia oppure la maschera del nome della minaccia (in base alla classificazione dell'Enciclopedia di virus) all'area attendibile.

È ad esempio possibile che si utilizzi frequentemente un programma di amministrazione remota, si tratta di un sistema di accesso remoto che consente di utilizzare le risorse da un computer remoto. Kaspersky Anti-Virus rileva questo tipo di attività come potenzialmente pericolose e potrebbe bloccarle. Per evitare di bloccare l'applicazione, è necessario creare una regola di esclusione per specificare Remote Admin come verdetto.

L'aggiunta di un'esclusione comporta la creazione di una regola che può essere utilizzata da diversi componenti dell'applicazione (Anti-Virus File, Anti-Virus Posta, Difesa Proattiva, Web Anti-Virus), e attività di scansione anti-virus.

➨ *Per creare una regola di esclusione, eseguire le operazioni seguenti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Esclusioni**, cliccare sul pulsante **Area attendibile**.
4. Nella finestra visualizzata, sulla scheda **Regole di esclusione**, cliccare sul pulsante **Aggiungi**.
5. Nella finestra **Maschera di esclusione** visualizzata, sezione **Proprietà**, selezionare un tipo di esclusione. Quindi, nella sezione **Descrizione della regola**, assegnare i valori ai tipi di esclusione selezionati e scegliere i componenti da includere nella regola.

Per creare una regola di esclusione dalla finestra dei rapporti, eseguire le seguenti operazioni:

1. Selezionare l'oggetto nel rapporto da aggiungere alle esclusioni.
2. Selezionare la voce **Aggiungi a zona attendibile** dal menu di scelta rapida dell'oggetto specificato.
3. Viene visualizzata la finestra **Maschera di esclusione**. Verificare di aver selezionato le impostazioni delle regole di esclusione desiderate. I campi relativi al nome dell'oggetto e al tipo di minaccia pertinente vengono compilati automaticamente in base ai dati del rapporto. Per creare la regola, cliccare sul pulsante **OK**.

ULTERIORI IMPOSTAZIONI DI ESCLUSIONE

È possibile imporre ulteriori condizioni di applicazione delle regole per alcuni oggetti in base al tipo di minaccia. Ad esempio, può essere necessario specificare impostazioni avanzate nei casi seguenti:

- *Invasore (intrusione nei processi delle applicazioni)*. Per questo tipo di minaccia, è possibile assegnare un nome, una maschera o il percorso completo dell'oggetto incorporato, ad esempio un file .dll, come condizione di esclusione aggiuntiva.
- *Avvio del browser Internet (avvio del browser con determinate impostazioni)*. Per questo tipo di minaccia, è possibile specificare le impostazioni di avvio del browser come impostazioni di esclusione aggiuntive. Ad esempio, è possibile impedire l'apertura dei browser con determinate impostazioni durante l'analisi delle applicazioni con Difesa Proattiva. Tuttavia, è necessario consentire l'apertura del dominio *www.kaspersky.com* nel browser con un collegamento da Microsoft Office Outlook, come regola di esclusione. A tale scopo, nella finestra **Maschera di esclusione** specificare l'applicazione Microsoft Office Outlook come **Oggetto** di esclusione, l'avvio del browser Internet come **Tipo di minaccia** e immettere una maschera di dominio consentita nel campo **Commento**.

MASCHERE DI ESCLUSIONE FILE CONSENTITE

Di seguito vengono illustrati in modo dettagliato alcuni esempi di maschere consentite che è possibile utilizzare per la creazione dell'elenco di file da escludere dalla scansione:

1. Maschere senza percorsi file:
   - ***.exe** – tutti i file con l'estensione *.exe*;
   - ***.ex?** – tutti i file con l'estensione *ex?* , in cui *?* può rappresentare un qualsiasi carattere singolo;
   - **test** – tutti i file con il nome *test.*
2. Maschere con percorsi file assoluti:
   - **C:\dir*.*** o **C:\dir*** o **C:\dir** – tutti i file contenuti nella cartella *C:\dir*;
   - **C:\dir*.exe** – tutti i file con l'estensione .exe contenuti nella cartella *C:\dir*;
   - **C:\dir*.ex?** – tutti i file con l'estensione *ex?* contenuti nella cartella *C:\dir*, dove *?* può rappresentare qualsiasi carattere;
   - **C:\dir\test** – solo il file con il nome *C:\dir\test.*

   Se non si desidera che l'applicazione esegua la scansione dei file in tutte le sottocartelle nidificate della cartella specificata, selezionare la casella ☑ **Includi sottocartelle** durante la creazione della maschera.
3. Maschere con percorsi file:
   - **dir*.*** o **dir*** o **dir** – tutti i file contenuti in tutte le cartelle *dir*;
   - **dir\test** – tutti i file *test* contenuti nelle cartelle *dir*;

- **dir*.exe** – tutti i file con l'estensione *.exe* contenuti in tutte le cartelle *dir*\;
- **dir*.ex?** – tutti i file con l'estensione *ex?* in tutte le cartelle *dir*\, in cui *?* può rappresentare qualsiasi carattere.

  Se non si desidera che l'applicazione esegua la scansione dei file in tutte le sottocartelle nidificate della cartella specificata, selezionare la casella **Includi sottocartelle** durante la creazione della maschera.

Le maschere di esclusione *.* e * possono essere utilizzate solo se si specifica il tipo di classificazione della minaccia indicato nella Virus Encyclopedia. In questo caso la minaccia specificata non verrà rilevata in alcun oggetto. L'uso di queste maschere senza specificare una classificazione in sostanza disabilita il monitoraggio. Inoltre, durante l'impostazione di un'esclusione, non è consigliabile selezionare un percorso relativo a un disco di rete creato in base a una cartella del file system attraverso il comando subst, nonché a un disco che rispecchia una cartella di rete. Potrebbe accadere infatti che a risorse diverse venga assegnato lo stesso nome del disco per utenti diversi, con l'inevitabile conseguenza di attivare in modo errato le regole di esclusione.

VEDERE ANCHE

Maschere di esclusione consentite secondo la Virus Encyclopedia 154

MASCHERE DI ESCLUSIONE CONSENTITE SECONDO LA VIRUS ENCYCLOPEDIA

Quando si aggiungono maschere per escludere determinate minacce in base alla relativa classificazione in Virus Encyclopedia, è possibile specificare le impostazioni seguenti:

- il nome completo della minaccia come indicato nella Virus Encyclopedia all'indirizzo www.viruslist.com, ad esempio **not-a-virus:RiskWare.RemoteAdmin.RA.311** o **Flooder.Win32.Fuxx**;
- Il nome della minaccia in base alla maschera, ad esempio:
  - **not-a-virus*** – esclude i programmi legittimi ma potenzialmente pericolosi dalla scansione, oltre ai programmi joke;
  - ***Riskware.*** – esclude il riskware dalla scansione;
  - ***RemoteAdmin.*** – esclude tutti i programmi di amministrazione remota dalla scansione.

VEDERE ANCHE

Maschere di esclusione file consentite 153

CREAZIONE DELL'ELENCO DI APPLICAZIONI ATTENDIBILI

È possibile creare un elenco di applicazioni attendibili. L'attività di tali programmi (inclusi l'attività sospetta, l'attività dei file, l'attività di rete e i tentativi di accesso al registro di sistema) non verrà controllata.

È ad esempio possibile ritenere che gli oggetti utilizzati in **Blocco note** di Microsoft Windows siano sicuri e non necessitino di scansione. In altre parole, si considera affidabile quest'applicazione. Per escludere dalla scansione gli oggetti utilizzati da questo processo, aggiungere l'applicazione **Blocco note** all'elenco delle applicazioni attendibili. Il file eseguibile e il processo dell'applicazione attendibile saranno contemporaneamente sottoposti a scansione anti-virus come in precedenza. Per escludere completamente l'applicazione dalla scansione, è necessario utilizzare le regole di esclusione (per ulteriori informazioni, consultare la sezione "Creazione di una regola di esclusione" a pagina 152).

Inoltre, determinate azioni classificate come pericolose potrebbero essere ritenute normali da diverse applicazioni. Le applicazioni che ad esempio commutano automaticamente le tastiere, come Punto Switcher, intercettano regolarmente il testo immesso sulla tastiera. Per tenere conto delle caratteristiche specifiche di tali applicazioni e disabilitare il monitoraggio delle relative attività, è consigliabile aggiungerle all'elenco delle applicazioni attendibili.

L'utilizzo dell'elenco di esclusione delle applicazioni attendibili consente inoltre di risolvere i potenziali conflitti di compatibilità tra Kaspersky Anti-Virus e altre applicazioni (ad esempio, traffico di rete da un altro computer già esaminato dall'applicazione anti-virus) e di potenziare la produttività del computer, particolarmente importante quando si utilizzano applicazioni server.

Per impostazione predefinita, Kaspersky Anti-Virus esamina gli oggetti aperti, eseguiti o salvati da qualsiasi processo di programma e monitora l'attività di tutte le applicazioni e il traffico di rete che creano.

➡ *Per aggiungere un'applicazione all'elenco delle applicazioni attendibili, eseguire le operazioni seguenti:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Esclusioni**, cliccare sul pulsante **Area attendibile**.
4. Nella finestra visualizzata, sulla scheda **Applicazioni attendibili**, cliccare sul pulsante **Aggiungi**.
5. Nella finestra **Applicazione attendibile** visualizzata, selezionare il programma cliccando sul pulsante **Sfoglia**. Viene aperto un menu di scelta rapida dal quale, cliccando su **Sfoglia**, si accede alla finestra standard di selezione file per selezionare il percorso del file eseguibile; oppure cliccando su **Applicazioni**, è possibile passare all'elenco delle applicazioni attualmente in esecuzione e selezionarne una o più, secondo necessità. Specificare le impostazioni necessarie per l'applicazione selezionata.

ESPORTAZIONE/IMPORTAZIONE DI COMPONENTI DI AREA ATTENDIBILE

Con le funzioni di importazione ed esportazione, è possibile trasferire le regole di esclusione e gli elenchi di applicazioni attendibili su altri computer.

➡ *Per copiare le regole di esclusione, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Esclusioni**, cliccare sul pulsante **Area attendibile**.
4. Nella finestra visualizzata, sulla scheda **Regole di esclusione**, cliccare sui bottoni **Esporta** o **Importa** per copiare le regole.

➡ *Per copiare l'elenco di applicazioni attendibili, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Esclusioni**, cliccare sul pulsante **Area attendibile**.
4. Nella finestra visualizzata, sulla scheda **Applicazioni attendibili**, cliccare sui bottoni **Esporta** o **Importa** per copiare l'elenco.

ESPORTAZIONE/IMPORTAZIONE DELLE IMPOSTAZIONI DI KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus consente di importare ed esportare le proprie impostazioni.

Questa funzione è utile, ad esempio, quando l'applicazione è installata sia nel computer di casa che in quello dell'ufficio. È possibile configurare le impostazioni preferite del programma sul computer di casa, esportarle sotto forma di file su un disco e, servendosi della funzione di importazione, caricarle sul computer in ufficio. Le impostazioni vengono salvate in uno speciale file di configurazione.

Per esportare le impostazioni correnti dell'applicazione, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazionidell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Gestione impostazioni di applicazione** cliccare sul pulsante **Salva**.
4. Nella finestra visualizzata, immettere il nome del file di configurazione e il percorso in cui salvarlo.

Per importare le impostazioni dell'applicazione da un file di configurazione salvato, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Gestione impostazioni di applicazione** cliccare sul pulsante **Importa**.
4. Nella finestra visualizzata, selezionare il file da cui importare le impostazioni di Kaspersky Anti-Virus.

RIPRISTINO DELLE IMPOSTAZIONI PREDEFINITE

È sempre possibile ripristinare le impostazioni predefinite o consigliate di Kaspersky Anti-Virus. Tali impostazioni consentono infatti di ottenere una configurazione ottimale e sono pertanto consigliate da Kaspersky Lab. Configurazione guidata dell'applicazione consente di ripristinare le impostazioni predefinite.

Nella finestra visualizzata, verrà chiesto di stabilire quali impostazioni salvare durante il ripristino del livello di protezione consigliato e per quali componenti.

L'elenco mostra i componenti di Kaspersky Anti-Virus le cui impostazioni sono diverse da quelle predefinite perché modificate dall'utente o perché accumulate dall'applicazione durante l'addestramento (Firewall o Anti-Spam). Se sono state create impostazioni speciali per uno o più componenti, anche queste verranno visualizzate nell'elenco.

Esempi di impostazioni speciali includono: elenchi di frasi e indirizzi consentiti e bloccati utilizzati da Anti-Spam, elenchi di indirizzi e di numeri di telefono ISP attendibili utilizzati dai componenti Web Anti-Virus e Anti-Spy, regole di esclusione create per i componenti dell'applicazione e regole di filtraggio delle applicazioni e dei pacchetti di Firewall.

Tali elenchi vengono popolati con l'utilizzo progressivo del programma, in base alle singole attività e ai requisiti di protezione, e la loro creazione spesso richiede molto tempo. Pertanto, si consiglia di salvarli quando si reimpostano le impostazioni dell'applicazione.

Al termine della Configurazione guidata, viene impostato il livello di protezione **Consigliato** per tutti i componenti, tranne che per le impostazioni che si è deciso di mantenere personalizzate durante il ripristino. Verranno inoltre applicate le impostazioni specificate durante l'esecuzione della procedura guidata.

Per ripristinare le impostazioni relative alla protezione, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Protezione**.
3. Nella sezione **Gestione impostazioni di applicazione**, cliccare sul pulsante **Reimposta**.
4. Nella finestra visualizzata, selezionare le caselle relative alle impostazioni da salvare. Cliccare sul pulsante **Avanti**. Verrà avviata la configurazione guidata iniziale di cui sarà necessario seguire le indicazioni.

ANTI-VIRUS FILE

Le impostazioni del componente **Anti-Virus File** vengono raggruppate in questa finestra (per ulteriori informazioni, consultare la sezione "Protezione anti-virus del file system del computer" a pag. 45). Modificando le impostazioni dell'applicazione, è possibile:

- modificare il livello di sicurezza (vedere a pag. 47);
- modificare l'azione da eseguire sugli oggetti rilevati (vedere pagina 48);
- creare un ambito di protezione (vedere a pag. 49);
- ottimizzare la scansione (vedere a pag. 50);
- configurare la scansione di file compositi (vedere a pag. 51);
- modificare la modalità di scansione (vedere a pag. 52);
- utilizzare l'analisi euristica (vedere a pag. 50);
- sospendere il componente (vedere a pag. 53);
- selezionare una tecnologia di scansione (vedere a pag. 52);
- ripristinare le impostazioni di protezione predefinite (vedere pagina 54) nel caso fossero state modificate;
- disabilitare Anti-Virus File.

Per disabilitare Anti-Virus File, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Anti-Virus File**.
3. Deselezionare la casella **Abilita Anti-Virus File** nella parte destra della finestra.

Per passare alle impostazioni di Anti-Virus File, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Anti-Virus File**.
3. Nella parte destra della finestra, selezionare le impostazioni del componente relative al livello di protezione e alla reazione alle minacce. Cliccare sul pulsante **Personalizza** per visualizzare le altre impostazioni di Anti-Virus File.

ANTI-VIRUS POSTA

Le impostazioni del componente **Anti-Virus Posta** vengono raggruppate in questa finestra (per ulteriori informazioni, consultare la sezione "Anti-Virus Posta" a pagina 56). Modificando le impostazioni dell'applicazione, è possibile:

- modificare il livello di sicurezza (vedere a pag. 58);
- modificare l'azione da eseguire sugli oggetti rilevati (vedere pagina 59);
- creare un ambito di protezione (vedere a pag. 60);
- modificare i metodi di scansione (vedere pagina 60);

- utilizzare l'analisi euristica (vedere a pag. 62);
- configurare la scansione di file compositi (vedere a pag. 63);
- configurare le condizioni di filtraggio degli oggetti allegati al messaggio di posta elettronica (vedere pagina 63);
- ripristinare le impostazioni di protezione predefinite (vedere pagina 64);
- disabilitare Anti-Virus Posta.

Per disabilitare Anti-Virus Posta, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Anti-Virus Posta**.
3. Deselezionare la casella **Abilita Anti-Virus Posta** nella parte destra della finestra.

Per passare alle impostazioni di Anti-Virus Posta, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Anti-Virus Posta**.
3. Nella parte destra della finestra, selezionare le impostazioni del componente relative al livello di protezione e alla reazione alle minacce. Cliccare sul pulsante **Personalizza** per visualizzare le altre impostazioni di Anti-Virus Posta.

ANTI-VIRUS WEB

Le impostazioni del componente **Web Anti-Virus** vengono raggruppate in questa finestra (per ulteriori informazioni, consultare la sezione "Web Anti-Virus" a pagina 66). Modificando le impostazioni dell'applicazione, è possibile:

- modificare il livello di sicurezza (vedere a pag. 68);
- modificare l'azione da eseguire sugli oggetti rilevati (vedere pagina 68);
- creare un ambito di protezione (vedere a pag. 69);
- modificare i metodi di scansione (vedere pagina 69);
- ottimizzare la scansione (vedere a pag. 70);
- utilizzare l'analisi euristica (vedere a pag. 70);
- ripristinare le impostazioni predefinite di Web Anti-Virus (vedere pagina 71);
- disabilitare Web Anti-Virus.

Per disabilitare Anti-Virus Web, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Web Anti-Virus**.
3. Deselezionare la casella **Abilita Web Anti-Virus** nella parte destra della finestra.

Per passare alle impostazioni di Anti-Virus Web, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazionidell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Web Anti-Virus**.

3. Nella parte destra della finestra, selezionare le impostazioni del componente relative al livello di protezione e alla reazione alle minacce. Cliccare sul pulsante **Personalizza** per visualizzare le altre impostazioni di Web Anti-Virus.

DIFESA PROATTIVA

Le impostazioni del componente **Difesa Proattiva** vengono raggruppate in questa finestra (per ulteriori informazioni, consultare la sezione "Difesa Proattiva" a pagina 73). Modificando le impostazioni dell'applicazione, è possibile:

- gestire l'elenco (vedere pagina 75) delle attività pericolose;
- modificare la risposta dell'applicazione alle attività pericolose (vedere pagina 75) nel sistema;
- monitorare gli account utente del sistema (vedere pagina 76);
- gestire l'elenco (vedere pagina 79) delle regole di monitoraggio del registro di sistema;
- creare regole per il monitoraggio degli oggetti di registro (vedere pagina 81);
- creare gruppi di oggetti di registro del sistema da monitorare (vedere pagina 80);
- disabilitare Analisi Attività Applicazione (vedere pagina 74) e i moduli Controllo del Registro (vedere pagina 79);
- disabilitare Difesa Proattiva.

Per disabilitare Difesa Proattiva, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Difesa Proattiva**.

3. Nella parte destra della finestra, deselezionare la casella **Abilita Difesa Proattiva**.

*Per disabilitare **Analisi Attività Applicazione** o **Controllo del Registro**, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Difesa Proattiva**.

3. Nella parte destra della finestra, deselezionare le caselle **Abilita Analisi Attività Applicazione** o **Abilita Controllo del Registro**.

Per procedere alla modifica delle impostazioni di Difesa Proattiva, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Difesa Proattiva**.

3. Nella parte destra della finestra, sezione **Analisi Attività Applicazione** oppure sezione **Controllo del Registro**, cliccare sul pulsante **Impostazioni**.

ANTI-SPY

Le impostazioni del componente **Anti-Spy** vengono raggruppate in questa finestra (per ulteriori informazioni, consultare la sezione "Anti-Spy" a pagina 83). Modificando le impostazioni dell'applicazione, è possibile:

- creare l'elenco di indirizzi di banner consentiti (vedere pagina 84);
- creare l'elenco di indirizzi di banner bloccati (vedere pagina 84);
- esportare/importare elenchi di indirizzi di banner (vedere pagina 85);
- creare l'elenco di numeri attendibili (vedere pagina 86);
- disabilitare i moduli Anti-Banner (vedere pagina 83) e Anti-Dialer (vedere pagina 86);
- disabilitare Anti-Spy.

Per disabilitare Anti-Spy, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Anti-Spy**.
3. Nella parte destra della finestra, deselezionare la casella **Abilita Anti-Spy**.

*Per disabilitare **Anti-Banner** o **Anti-Dialer**, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Anti-Spy**.
3. Nella parte destra della finestra, deselezionare la casella **Abilita Anti-Banner** (**Abilita Anti-Dialer**).

Per procedere alla modifica delle impostazioni di Anti-Spy, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazionidell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Anti-Spy**.
3. Nella parte destra della finestra, sezione **Anti-Banner** oppure sezione **Anti-Dialer**, cliccare sul pulsante **Impostazioni**.

ANTI-HACKER

Le impostazioni del componente **Anti-Hacker** vengono raggruppate in questa finestra (per ulteriori informazioni, consultare la sezione "Protezione dagli attacchi di rete" a pagina 87). Modificando le impostazioni dell'applicazione, è possibile:

- modificare il livello di protezione di Anti-Hacker (vedere pagina 89);
- creare le regole per le applicazioni manualmente (vedere pagina 90) e mediante un modello (vedere pagina 91);
- creare regole per i filtri pacchetti (vedere pagina 92);
- modificare la priorità delle regole (vedere pagina 92);
- esportare/importare le regole (vedere pagina 93);
- ottimizzare le regole per le applicazioni e i pacchetti (vedere pagina 93);
- creare regole per le aree di protezione (vedere pagina 96);
- modificare lo stato delle aree di protezione (vedere pagina 98);

- abilitare/disabilitare la modalità mascheramento (vedere pagina 98);
- modificare la modalità Firewall (vedere pagina 98);
- disabilitare i moduli Firewall e Sistema rilevamento intrusioni (vedere pagina 99);
- disabilitare Anti-Hacker.

➡ *Per disabilitare Anti-Hacker, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Selezionare la sezione **Anti-Hacker** nella parte sinistra della finestra.
3. Deselezionare la casella ☑ **Abilita Anti-Hacker** nella parte destra della finestra.

➡ *Per disabilitare **Firewall** o **Sistema rilevamento intrusioni**, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Selezionare la sezione **Anti-Hacker** nella parte sinistra della finestra.
3. Deselezionare la casella ☑ **Abilita Firewall** oppure la casella ☑ **Abilita Sistema rilevamento intrusioni** nella parte destra della finestra.

➡ *Per procedere alla modifica delle impostazioni di Anti-Hacker, eseguire le seguenti operazioni:*

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Selezionare la sezione **Anti-Hacker** nella parte sinistra della finestra.
3. Nella parte destra della finestra, cliccare sul pulsante **Impostazioni** nella sezione **Firewall**.

ANTI-SPAM

Le impostazioni del componente **Anti-Spam** vengono raggruppate in questa finestra (per ulteriori informazioni, consultare la sezione "Anti-Spam" a pagina 103). Modificando le impostazioni dell'applicazione, è possibile:

- modificare il livello di riservatezza (vedere pagina 109);
- utilizzare Recapito posta (vedere pagina 109);
- escludere i messaggi di Microsoft Exchange Server dalla scansione (vedere pagina 110);
- modificare i metodi di scansione (vedere pagina 111);
- selezionare la tecnologia di filtraggio dello spam (vedere pagina 111);
- definire i fattori di spam e spam potenziale (vedere pagina 112);
- utilizzare ulteriori funzioni di filtraggio dello spam (vedere pagina 112);
- creare l'elenco di mittenti consentiti (vedere pagina 113);
- creare l'elenco di frasi di consentite (vedere pagina 114);
- importazione l'elenco di mittenti consentiti (vedere pagina 114);
- creare l'elenco di mittenti bloccati (vedere pagina 115);

- creare l'elenco di frasi di bloccate (vedere pagina 116);
- configurare l'elaborazione dello spam in Microsoft Office Outlook (vedere pagina 117), Microsoft Outlook Express (Windows Mail) (vedere pagina 118), The Bat! (vedere pagina 119);
- addestrare Anti-Spam mediante Apprendimento guidato (vedere pagina 106), sui messaggi di posta elettronica in uscita (vedere pagina 107),sull'utilizzo di un client di posta (vedere pagina 107), con rapporti (vedere pagina 108);
- disabilitare Anti-Spam.

Per disabilitare Anti-Spam, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Anti-Spam**.
3. Deselezionare la casella **Abilita Anti-Spam** nella parte destra della finestra.

Per procedere alla modifica delle impostazioni di Anti-Spam, eseguire le operazioni seguenti:

1. Aprire Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Anti-Spam**.
3. Nella parte destra della finestra, sezione **Riservatezza**, cliccare sul pulsante **Personalizza**.

SCANSIONE

La selezione del metodo da utilizzare per la scansione degli oggetti presenti nel computer viene determinata da un set di proprietà assegnato a ogni attività.

Gli specialisti di Kaspersky Lab distinguono diverse attività di scansione anti-virus. Le più comuni sono le seguenti:

Scansione

Esame degli oggetti selezionati dall'utente. È possibile esaminare qualsiasi oggetto nel file system del computer.

Scansione completa

Scansione approfondita dell'intero sistema. Gli oggetti seguenti vengono esaminati per impostazione predefinita: memoria di sistema, programmi caricati all'avvio, backup di sistema, database di posta, dischi rigidi, unità rimovibili e unità di rete.

Scansione rapida

Scansione anti-virus degli oggetti di avvio del sistema operativo.

La finestra delle impostazioni di ciascun attività consente di eseguire le seguenti operazioni:

- selezionare il livello di sicurezza (vedere pagina 127) con le impostazioni che verranno utilizzate dall'attività;
- selezionare un'azione (vedere pagina 127) applicata quando si rileva un oggetto infetto / potenzialmente infetto;
- creare una pianificazione (vedere pagina 132) per l'esecuzione automatica delle attività;
- specificare i tipi di file (vedere pagina 129) da sottoporre a scansione anti-virus;
- specificare le impostazioni di scansione dei file compositi (vedere pagina 130);

- selezionare i metodi di scansione e le tecnologie di scansione (vedere pagina 130);
- assegnare impostazioni di scansione comuni a tutte le attività (vedere pagina 134).

Per modificare le impostazioni dell'attività, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Scansione** (**Scansione completa**, **Scansione rapida**).
3. Nella parte destra della finestra, selezionare il livello di sicurezza necessario, la risposta alla minaccia, quindi configurare la modalità di esecuzione. Cliccare sul pulsante **Personalizza** per visualizzare le altre impostazioni dell'attività. Per ripristinare le impostazioni predefinite, cliccare sul pulsante **Livello predefinito**.

AGGIORNAMENTO

L'aggiornamento di Kaspersky Anti-Virus viene eseguito mediante le impostazioni che determinano quanto segue:

- l'origine (vedere pagina 137) da cui verranno scaricati e installati gli aggiornamenti;
- la modalità di esecuzione dell'aggiornamento (vedere pagina 140) e i componenti specifici da aggiornare (vedere pagina 141);
- la frequenza di avvio degli aggiornamenti in caso di avvio pianificato configurato (vedere pagina 139);
- l'account (vedere pagina 139) con cui avviare l'aggiornamento;
- se gli aggiornamenti devono essere copiati in un'origine locale (vedere pagina 141);
- l'utilizzo di un server proxy (vedere pagina 138).

Per procedere con la configurazione dell'aggiornamento, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Aggiornamento**.
3. Selezionare la modalità di esecuzione necessaria nella parte destra della finestra. Cliccare sul pulsante **Configura** per passare alla configurazione di altre attività.

OPZIONI

Nella finestra **Opzioni** è possibile utilizzare le funzioni avanzate di Kaspersky Anti-Virus elencate di seguito:

- Auto-difesa dell'applicazione (vedere pagina 164).
- Limitazione dell'accesso all'applicazione (vedere pagina 164).
- Utilizzo dell'applicazione su un laptop (vedere pagina 165).
- Limitazione delle dimensioni dei file iSwift (vedere pagina 165).
- Notifiche sugli eventi Kaspersky Anti-Virus (vedere pagina 165):
  - selezione del tipo di eventi e modalità di invio delle notifiche (vedere pagina 166);
  - configurazione della notifica di posta elettronica (vedere pagina 167);

- configurazione del registro di eventi (vedere pagina 167).

- Elementi attivi dell'interfaccia (vedere pagina 167).

AUTO-DIFESA DELL'APPLICAZIONE

Kaspersky Anti-Virus garantisce la protezione del computer da programmi malware e, proprio per questo, può essere essa stessa oggetto di attacchi da parte di tali programmi che cercano di bloccarne l'attività o eliminarla.

Per garantire la stabilità del sistema di protezione del computer, l'applicazione dispone di propri meccanismi di auto-difesa e di protezione dall'accesso remoto.

Nei computer che utilizzano sistemi operativi a 64 bit e Microsoft Windows Vista, l'auto-difesa è disponibile solo per impedire la modifica o l'eliminazione dei file di Kaspersky Anti-Virus sui dischi locali e delle relative voci del Registro di sistema.

Quando la protezione da accessi remoti è abilitata, in alcuni casi è possibile che sia necessario consentire i programmi di amministrazione remota (ad esempio RemoteAdmin) per gestire l'applicazione. A tale scopo, è necessario aggiungere tali programmi all'elenco di applicazioni attendibili e abilitare l'impostazione **Disabilita analisi attività applicazione** per questi.

Per abilitare il meccanismo di auto-difesa di Kaspersky Anti-Virus, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Auto-Difesa**, selezionare la casella **Abilita Auto-Difesa** per distribuire il meccanismo di protezione di Kaspersky Anti-Virus dalle modifiche o dall'eliminazione dei file del disco rigido, dei processi della RAM e delle voci del Registro di sistema.

   Nella sezione **Auto-Difesa**, selezionare la casella **Disabilita controllo esterno del servizio di sistema** per bloccare qualsiasi tentativo di gestire i servizi dell'applicazione in remoto.

   Se si tenta di eseguire una delle azioni elencate, verrà visualizzato un messaggio sopra l'icona dell'applicazione nell'area di notifica della barra delle applicazioni (sempre che il servizio di notifica non sia stato disabilitato dall'utente).

LIMITAZIONE DELL'ACCESSO ALL'APPLICAZIONE

Un personal computer può essere utilizzato da diversi utenti, con differenti livelli di esperienza in ambito informatico. Pertanto, lasciare libero accesso a Kaspersky Anti-Virus e alle relative impostazioni potrebbe ridurre notevolmente il livello di protezione del computer nel suo insieme.

Per aumentare il livello di protezione del computer, utilizzare una password per accedere a Kaspersky Anti-Virus. In questo modo, è possibile che vengano bloccate tutte le operazioni, ad eccezione delle notifiche di rilevamento di oggetti pericolosi e viene impedita l'esecuzione delle seguenti azioni:

- modifica delle impostazioni dell'applicazione;
- chiusura dell'applicazione;
- disabilitazione dei componenti di protezione e delle attività di scansione;
- disabilitazione dei criteri (quando l'applicazione viene eseguita mediante Kaspersky Administration Kit);
- rimozione dell'applicazione.

Ognuna delle azioni sopra descritte comporta un abbassamento del livello di protezione del computer, quindi tentare di stabilire gli utenti del computer autorizzati a intraprendere tali azioni.

Per proteggere l'accesso all'applicazione con una password, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Protezione tramite password**, selezionare la casella **Abilita protezione tramite password** e cliccare sul pulsante **Impostazioni**.
4. Nella finestra **Protezione tramite password** visualizzata, immettere la password e specificare l'area da includere nella limitazione di accesso. In questo modo, ogni volta che un utente del computer cercherà di eseguire le azioni selezionate dovrà immettere una password.

UTILIZZO DELL'APPLICAZIONE SU UN LAPTOP

Per risparmiare energia (carica della batteria) su un computer portatile, è possibile rimandare le attività di scansione e aggiornamento.

Poiché sia la scansione anti-virus di un computer che l'aggiornamento dell'applicazione richiedono una notevole quantità di risorse e di tempo, è consigliabile disabilitare l'avvio pianificato di tali attività. In questo modo si prolunga la durata della batteria. Se necessario, è possibile aggiornare l'applicazione o avviare una scansione anti-virus manualmente.

Per utilizzare il servizio di risparmio energetico per funzionamento a batteria, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Risorse**, selezionare la casella **Disabilita attività pianificate se l'alimentazione è a batteria**.

LIMITAZIONE DELLE DIMENSIONI DEI FILE ISWIFT

I *file iSwift* contengono informazioni sugli oggetti NTFS già sottoposti a una scansione anti-virus (con tecnologia iSwift). L'utilizzo di tali file consente di velocizzare la scansione, poiché Kaspersky Anti-Virus esamina soltanto gli oggetti modificati dall'ultima scansione. Col tempo, le dimensioni dei file iSwift aumentano. Si consiglia di limitare le dimensioni di tali file. Una volta raggiunto il valore specificato, il file iSwift verrà cancellato.

Per limitare le dimensioni dei file iSwift, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Risorse**, selezionare la casella **Reimposta database iSwift quando raggiunge** e specificare la dimensione del database in MB.

NOTIFICHE DEGLI EVENTI DI KASPERSKY ANTI-VIRUS

Durante il funzionamento di Kaspersky Anti-Virus. si verificano diversi tipi di eventi, che possono essere di riferimento o contenere dati importanti. Un evento può ad esempio informare l'utente del completamento con esito positivo di un aggiornamento dell'applicazione o registrare un errore nel funzionamento di un determinato componente che deve essere eliminato immediatamente.

Per essere aggiornati sugli eventi più recenti che si verificano durante il funzionamento di Kaspersky Anti-Virus, utilizzare la funzione di notifica.

Le notifiche possono essere inviate in uno dei seguenti modi:

- messaggi a comparsa che vengono visualizzati sopra l'icona dell'applicazione nell'area di notifica;
- notifica acustica;
- messaggi di posta elettronica;
- registrazione di informazioni nel registro eventi.

Per utilizzare il servizio di notifica, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Aspetto**, selezionare la casella **Abilita notifiche** e cliccare sul pulsante **Impostazioni**.
4. Nella finestra **Impostazioni notifica** visualizzata, specificare i tipi di eventi Kaspersky Anti-Virus di cui si desidera ricevere notifiche e i tipi di notifiche.

VEDERE ANCHE

Selezione del tipo di evento e della modalità di invio delle notifiche 166

Configurazione della notifica tramite posta elettronica 167

Configurazione del registro eventi 167

SELEZIONE DEL TIPO DI EVENTO E DELLA MODALITÀ DI INVIO DELLE NOTIFICHE

Durante il funzionamento di Kaspersky Anti-Virus, si verificano i tipi di eventi seguenti:

- Le **notifiche critiche** sono eventi di una certa rilevanza. Si consiglia vivamente di segnalarle con le notifiche poiché fanno riferimento a problemi di funzionamento dell'applicazione o vulnerabilità della protezione del computer, ad esempio *database obsoleti* o *periodo di validità della licenza scaduto*.
- Le **notifiche errori** sono eventi che causano l'interruzione del funzionamento dell'applicazione, ad esempio *database mancanti o danneggiati*.
- Le **notifiche importanti** sono eventi cui l'utente deve prestare attenzione poiché riflettono situazioni importanti nel funzionamento dell'applicazione, ad esempio *database obsoleti* o *prossima scadenza della licenza*.
- Le **notifiche minori** sono messaggi di riferimento che in linea generale non contengono informazioni importanti, ad esempio *oggetti in quarantena*.

Per specificare quali eventi notificare all'utente e le modalità di notifica, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Aspetto**, selezionare la casella **Abilita notifiche** e cliccare sul pulsante **Impostazioni**.
4. Nella finestra **Impostazioni notifica** visualizzata, selezionare le caselle relative agli eventi di cui si desidera ricevere notifiche e le modalità di invio delle notifiche.

CONFIGURAZIONE DELLA NOTIFICA TRAMITE POSTA ELETTRONICA

Dopo aver selezionato gli eventi (per ulteriori informazioni, consultare la sezione "Selezione del tipo di evento e della modalità di invio delle notifiche" a pagina 166) di cui si desidera ricevere una notifica tramite posta elettronica, è necessario impostare le notifiche.

Per configurare le notifiche tramite posta elettronica, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Aspetto**, selezionare la casella **Abilita notifiche** e cliccare sul pulsante **Impostazioni**.
4. Nella finestra **Impostazioni notifica** visualizzata, selezionare le caselle relative agli eventi desiderati nel campo **Email** e cliccare sul pulsante **Impostazioni posta elettronica**.
5. Nella finestra **Impostazioni di notifica e-mail** visualizzata, specificare i valori necessari per le impostazioni. Per inviare notifiche sugli eventi a orari stabiliti, creare una pianificazione per l'invio del messaggio informativo cliccando sul pulsante **Cambia**. Apportare le modifiche necessarie nella finestra **Pianifica** visualizzata.

CONFIGURAZIONE DEL REGISTRO EVENTI

Kaspersky Anti-Virus offre la possibilità di registrare le informazioni relative agli eventi che si verificano mentre l'applicazione è in esecuzione, nel registro eventi generale di Microsoft Windows (**Applicazione**) o in un registro eventi specifico per Kaspersky Anti-Virus (**Registro Eventi Kaspersky**).

È possibile visualizzare gli eventi in **Visualizzatore eventi** di Microsoft Windows, selezionabile da **Avvia/Impostazioni/Panello di controllo/Strumenti di amministrazione/Visualizza i registri eventi**.

Per configurare il registro eventi, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Nella sezione **Aspetto**, selezionare la casella **Abilita notifiche** e cliccare sul pulsante **Impostazioni**.
4. Nella finestra **Impostazioni notifica** visualizzata, selezionare le caselle relative agli eventi desiderati nel campo **Registro** e cliccare sul pulsante **Impostazioni registro**.
5. Nella finestra **Impostazioni registro eventi** visualizzata, selezionare il registro in cui verranno registrate le informazioni sugli eventi.

ELEMENTI ATTIVI DELL'INTERFACCIA

Gli elementi attivi dell'interfaccia includono le seguenti opzioni di Kaspersky Anti-Virus:

Anima icona area di notifica della barra delle applicazioni.

L'icona dell'applicazione nell'area di notifica cambia in base all'operazione eseguita dall'applicazione. Ad esempio, durante la scansione dei messaggi di posta elettronica, viene visualizzata un'icona di lettera di piccole dimensioni di fronte all'icona dell'applicazione. Per impostazione predefinita, l'icona dell'applicazione è animata. In questo caso, l'icona mostra solo lo stato di protezione del computer: se la protezione è abilitata, l'icona è colorata, mentre se la protezione è sospesa o disabilitata, l'icona diventa grigia.

Mostra "Protected by Kaspersky Lab" nella schermata di accesso a Microsoft Windows.

Per impostazione predefinita, questo indicatore viene visualizzato nell'angolo superiore destro della schermata all'avvio di Kaspersky Anti-Virus e informa l'utente che il computer è protetto da qualsiasi tipo di minaccia.

> Se l'applicazione viene installata in un computer che utilizza Microsoft Windows Vista, questa opzione non è disponibile.

Per configurare gli elementi attivi dell'interfaccia, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Opzioni**.
3. Selezionare le caselle necessarie nella sezione **Aspetto**.

RAPPORTI E ARCHIVIAZIONI

La sezione contiene le impostazioni che consentono di controllare le operazioni con i file di dati dell'applicazione.

I file di dati dell'applicazione sono oggetti messi in quarantena da Kaspersky Anti-Virus o spostati nella cartella Backup, nonché file contenenti rapporti sul funzionamento dei componenti dell'applicazione.

In questa sezione, è possibile:

- configurare la creazione e l'archiviazione dei rapporti (vedere pagina 169);
- configurare la quarantena e il backup (vedere pagina 171);
- svuotare l'archivio dei rapporti, la quarantena e il backup.

Per svuotare le aree di archiviazione, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Rapporti e archiviazioni**.
3. Nella finestra visualizzata, cliccare sul pulsante **Cancella**.
4. Nella finestra **File di dati** visualizzata, specificare le aree di archiviazione da cui rimuovere tutti gli oggetti.

VEDERE ANCHE

Principi di gestione dei rapporti 169

Configurazione dei rapporti 169

Quarantena per oggetti potenzialmente infetti 170

Azioni sugli oggetti in quarantena 170

Copie di backup degli oggetti pericolosi 171

Utilizzo delle copie di backup 171

Configurazione della quarantena e del backup 171

PRINCIPI DI GESTIONE DEI RAPPORTI

Il funzionamento di ciascun componente di Kaspersky Anti-Virus e l'esecuzione di ciascuna attività di scansione anti-virus o aggiornamento vengono registrati in un rapporto.

Per visualizzare i rapporti, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Cliccare sul pulsante **Rapporto**.

Per verificare tutti gli eventi relativi al funzionamento di un componente o all'esecuzione di un'attività nel rapporto, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione e premere il pulsante **Rapporto**.
2. Nella finestra visualizzata, sulla scheda **Rapporto**, selezionare il nome di un componente o di un'attività, quindi cliccare sul collegamento **Dettagli**. Verrà visualizzata una finestra contenente informazioni dettagliate sulle prestazioni del componente o attività selezionati. Le statistiche relative alle prestazioni vengono visualizzate nella parte superiore della finestra; nelle varie schede poste nella parte centrale sono disponibili informazioni dettagliate. La composizione delle schede può variare in base al componente o all'attività.

Per importare il rapporto in un file di testo, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione e cliccare sul pulsante **Rapporto**.
2. Nella finestra visualizzata, sulla scheda **Rapporto**, selezionare il nome di un componente o di un'attività, quindi cliccare sul collegamento **Dettagli**.
3. Nella finestra visualizzata saranno disponibili le informazioni sulle prestazioni del componente o dell'attività selezionati. Premere il pulsante **Salva con nome** e specificare se si desidera salvare il file di rapporto.

CONFIGURAZIONE DEI RAPPORTI

È possibile modificare le seguenti impostazioni di creazione e salvataggio dei rapporti:

- Consentire o bloccare la registrazione degli eventi informativi. Solitamente, questi eventi non sono critici per la protezione (casella **Registra eventi non critici**).
- Consentire il salvataggio nel rapporto solo degli eventi che si sono verificati dall'ultimo avvio dell'attività. In questo modo è possibile limitare l'uso di spazio del disco riducendo le dimensioni del rapporto (casella **Mantieni solo eventi recenti**). Se la casella è selezionata, le informazioni verranno aggiornate ogni volta che l'attività viene riavviata. Tuttavia, verranno sovrascritte solo le informazioni non critiche.
- Impostare il termini di archiviazione per i rapporti (casella **Non memorizzare rapporti di oltre**). Per impostazione predefinita, la durata di memorizzazione degli oggetti è di 14 giorni. Una volta trascorso questo periodo, gli oggetti vengono eliminati. È possibile modificare la durata massima di archiviazione o persino rimuovere eventuali limiti imposti su tale valore.
- Specificare le dimensioni massime del rapporto (casella **Dimensione massima del file**). Per impostazione predefinita, la dimensione massima è di 100 MB. È possibile annullare eventuali restrizioni impostate sulla dimensione del rapporto o immettere un altro valore.

Per modificare le impostazioni di creazione e archiviazione, eseguire le seguenti operazioni:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Rapporti e archiviazioni**.

3. Nella sezione **Rapporto**, selezionare tutte le caselle necessarie, quindi impostare il termine di archiviazione e la dimensione massima del rapporto, secondo necessità.

QUARANTENA PER OGGETTI POTENZIALMENTE INFETTI

Quarantena è uno speciale repository in cui vengono memorizzati gli oggetti che potrebbero essere stati infettati da virus.

Gli **oggetti potenzialmente infetti** sono oggetti sospettati di essere stati infettati da virus o relative varianti.

Perché alcuni oggetti sono considerati come *potenzialmente infetti*? Non è sempre possibile determinare esattamente se un oggetto è infetto, per i seguenti probabili motivi:

- *Il codice dell'oggetto analizzato ricorda quello di una minaccia nota ma è in parte modificato*.

  I database dell'applicazione contengono informazioni sulle minacce al momento esaminate dagli specialisti di Kaspersky Lab. Se un programma dannoso è stato modificato e le modifiche non sono state ancora inserite nei database, Kaspersky Anti-Virus classifica l'oggetto infetto con il programma dannoso modificato come oggetto potenzialmente infetto e indica con esattezza la minaccia alla quale somiglia questa infezione.

- *La struttura del codice dell'oggetto rilevato ricorda un programma dannoso; tuttavia nei database dell'applicazione non è stato registrato nulla di simile*.

  È abbastanza probabile che si tratti di un nuovo tipo di minaccia, pertanto Kaspersky Anti-Virus classifica l'oggetto come oggetto potenzialmente infetto.

I file vengono identificati come potenzialmente infettati da un virus dall'*analisi euristica di codice*. Questo meccanismo è estremamente efficace e determina falsi positivi molto raramente.

Un oggetto potenzialmente infetto può essere rilevato e messo in quarantena mediante una scansione anti-virus oppure mediante Anti-Virus File, Anti-Virus Posta o Difesa Proattiva.

Quando un oggetto viene messo in Quarantena, viene spostato, non copiato. Esso viene eliminato dal disco o dalla posta elettronica e salvato nella cartella Quarantena. I file in Quarantena vengono salvati in un formato speciale e non sono pericolosi.

VEDERE ANCHE

Azioni sugli oggetti in quarantena..170

Configurazione della quarantena e del backup 171

AZIONI SUGLI OGGETTI IN QUARANTENA

È possibile eseguire le seguenti operazioni con gli oggetti in quarantena:

- mettere in quarantena i file sospettati di essere infetti;
- esaminare e disinfettare tutti gli oggetti potenzialmente infetti in quarantena utilizzando i database dell'applicazione correnti;
- ripristinare i file nelle cartelle da cui sono stati spostati per essere messi in quarantena oppure nelle cartelle selezionate dall'utente;
- eliminare tutti gli oggetti in quarantena oppure un gruppo di oggetti selezionati.

Per intraprendere azioni sugli oggetti in quarantena, eseguire le seguenti operazioni:

1. Aprire la finestra principalee cliccare sul collegamento **Rilevati**.
2. Nella finestra visualizzata, sulla scheda **Quarantena**, eseguire le azioni necessarie.

COPIE DI BACKUP DEGLI OGGETTI PERICOLOSI

In alcuni casi non è possibile mantenere l'integrità degli oggetti durante la disinfezione. Se il file disinfettato contiene informazioni importanti, e dopo la disinfezione diventa in parte o del tutto inaccessibile, è possibile provare a ripristinare l'oggetto originale dalla copia di backup.

La **copia di backup** è una copia dell'oggetto pericoloso originale creata quando l'oggetto è stato disinfettato o eliminato per la prima volta e salvata sotto forma di backup.

Backup è uno repository speciale che contiene copie di backup degli oggetti pericolosi dopo l'elaborazione o l'eliminazione. La principale funzione del backup è la possibilità di ripristinare in qualsiasi momento l'oggetto originale. I file del backup vengono salvati in un formato speciale e non costituiscono un pericolo.

VEDERE ANCHE

Utilizzo delle copie di backup 171

Configurazione della quarantena e del backup 171

UTILIZZO DELLE COPIE DI BACKUP

È possibile eseguire le seguenti operazioni con gli oggetti archiviati nel backup:

- ripristinare le copie selezionate;
- eliminare gli oggetti.

Per intraprendere azioni sugli oggetti del backup, eseguire le seguenti operazioni:

1. Aprire la finestra principalee cliccare sul collegamento **Rilevati**.
2. Nella finestra visualizzata, sulla scheda **Backup**, eseguire le azioni necessarie.

CONFIGURAZIONE DELLA QUARANTENA E DEL BACKUP

È possibile modificare le impostazioni seguenti per la quarantena e il backup:

- Abilitare la modalità Scansione automatica per gli oggetti in quarantena dopo ogni aggiornamento dei database dell'applicazione (casella **Scansiona file nella quarantena dopo l'aggiornamento**).

  Kaspersky Anti-Virus non è in grado di eseguire la scansione degli oggetti in quarantena subito dopo l'aggiornamento dei database dell'applicazione se tali oggetti sono in uso.

- Determinare la durata massima di archiviazione per gli oggetti in quarantena e le copie degli oggetti nel backup (casella **Memorizza oggetti non più di**). Per impostazione predefinita, la durata di archiviazione degli oggetti è di 30 giorni. Una volta trascorso questo periodo, gli oggetti vengono eliminati. È possibile modificare la durata massima di archiviazione o persino rimuovere eventuali limiti imposti su tale valore.

- Specificare la dimensione massima dell'area di archiviazione dei dati (casella **Dimensione massima del file**). Per impostazione predefinita, la dimensione massima è di 250 MB. È possibile annullare eventuali restrizioni impostate sulla dimensione del rapporto o immettere un altro valore.

Per configurare le impostazioni della quarantena e del backup:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Rapporti e archiviazioni**.
3. Nella sezione **Quarantena e Backup**, selezionare le caselle desiderate e specificare la dimensione massima dell'area di memorizzazione dei dati in base alle esigenze.

RETE

La sezione contiene impostazioni che consentono di:

- creare un elenco di porte da monitorare (vedere pagina 172);
- abilitare/disabilitare la modalità di scansione con connessione crittografata (mediante il protocollo SSL) (vedere pagina 173).

CREAZIONE DI UN ELENCO DI PORTE DA MONITORARE

Componenti della protezione come Anti-Virus Posta, Web Anti-Virus, Anti-Hacker e Anti-Spam controllano i flussi di dati trasferiti attraverso protocolli specifici e determinate porte del computer. Anti-Virus Posta, ad esempio, analizza le informazioni trasferite tramite il protocollo SMTP mentre Anti-Virus Web analizza i pacchetti HTTP.

È possibile selezionare una delle due modalità di monitoraggio delle porte:

- **Monitorare tutte le porte**.
- **Soltanto le porte selezionate**. Il pacchetto di installazione comprende un elenco delle porte utilizzate per trasmettere la posta elettronica e il traffico HTTP.

È possibile aggiungere una nuova porta o disabilitare il monitoraggio di una determinata porta, disabilitando quindi l'analisi del traffico che passa attraverso tale porta per individuare oggetti pericolosi.

Ad esempio, nel computer è presente una porta non standard attraverso la quale vengono scambiati dati con un computer remoto utilizzando il protocollo HTTP. Anti-Virus Web controlla il traffico HTTP. Per analizzare questo traffico allo scopo di individuare codice dannoso, è possibile aggiungere questa porta a un elenco di porte monitorate.

Quando viene avviato uno dei componenti, Kaspersky Anti-Virus apre la porta 1110 come porta di attesa per tutte le connessioni in arrivo. Se in quel momento la porta è riservata, seleziona la porta 1111, 1112 e così via come porta di attesa.

Se si utilizza Kaspersky Anti-Virus insieme al firewall di un altro fornitore, è necessario configurare il firewall in modo da consentire l'esecuzione di *avp.exe* (processo interno di Kaspersky Anti-Virus) su tutte le porte elencate in precedenza.

Ad esempio, il firewall contiene una regola per *iexplorer.exe* che consente la creazione di connessioni sulla porta 80. Tuttavia, quando Kaspersky Anti-Virus intercetta la query di connessione avviata da *iexplorer.exe* sulla porta 80, la trasferisce ad *avp.exe*, che a sua volta tenta di stabilire la connessione con la pagina Web in modo indipendente. Se non è disponibile una regola per *avp.exe*, il firewall blocca la query. L'utente non sarà quindi n grado di accedere alla pagina Web.

Per aggiungere una porta all'elenco delle porte monitorate:

1. Aprire la finestra delle impostazioni dell'applicazione.

2. Nella parte sinistra della finestra, selezionare la sezione **Rete**.
3. Nella sezione **Porte da monitorate**, cliccare sul pulsante **Impostazioni porta**.
4. Nella finestra **Impostazioni porta** visualizzata, cliccare sul pulsante **Aggiungi**.
5. Nella finestra **Porta** visualizzata, specificare i dati necessari.

Per escludere una porta dall'elenco di porte monitorate:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Rete**.
3. Nella sezione **Porte da monitorate**, cliccare sul pulsante **Impostazioni porta**.
4. Nella finestra **Impostazioni porta** visualizzata, deselezionare la casella accanto alla descrizione della porta.

SCANSIONE DELLE CONNESSIONI CRITTOGRAFATE

La connessione mediante il protocollo SSL (Secure Sockets Layer) consente di proteggere il canale di scambio dei dati in Internet. Il protocollo SSL consente di identificare le parti che scambiano i dati mediante certificati elettronici, codificando i dati trasferiti e garantendone l'integrità durante il trasferimento.

Queste funzioni del protocollo vengono utilizzate dai pirati informatici per diffondere programmi dannosi, poiché quasi tutti i programmi anti-virus non esaminano il traffico SSL.

Kaspersky Anti-Virus verifica le connessioni sicure utilizzando un certificato di Kaspersky Lab. Tale certificato verrà sempre utilizzato per controllare se la connessione è sicura.

Scansioni successive del traffico tramite il protocollo SSL verranno eseguite utilizzando il certificato di Kaspersky Lab installato. In caso di rilevamento di un certificato non valido durante la connessione al server, ad esempio se il certificato viene sostituito da un utente malintenzionato, verrà visualizzata una notifica in cui verrà richiesto di accettare o rifiutare il certificato oppure di visualizzarne le informazioni.

Per abilitare la scansione delle connessioni crittografate, eseguire le operazioni seguenti:

1. Aprire la finestra delle impostazioni dell'applicazione.
2. Nella parte sinistra della finestra, selezionare la sezione **Rete**.
3. Nella sezione **Connessioni crittografate**, selezionare la casella **Scansione delle connessioni crittografate** e cliccare sul pulsante **Installa certificato**.
4. Nella finestra visualizzata, cliccare sul pulsante **Installa certificato**. In questo modo viene avviata una procedura guidata che contiene le istruzioni da seguire per installare correttamente il certificato.

L'installazione automatica del certificato è disponibile solo in Microsoft Internet Explorer. Per esaminare le connessioni crittografate in Mozilla Firefox (vedere pagina174) e Opera (vedere pagina 174), è necessario installare un certificato Kaspersky Lab manualmente.

VEDERE ANCHE

Scansione delle connessioni crittografate in Mozilla Firefox 174

Scansione delle connessioni crittografate in Opera 174

SCANSIONE DELLE CONNESSIONI CRITTOGRAFATE IN MOZILLA FIREFOX

Il browser Mozilla Firefox non utilizza la memoria certificati di Microsoft Windows. Per eseguire la scansione delle connessioni SSL in Mozilla Firefox, è necessario installare il certificato di Kaspersky Lab manualmente.

➡ *Per installare il certificato di Kaspersky Lab, eseguire le operazioni seguenti:*

1. Nel menu del browser, selezionare la voce **Strumenti** → **Opzioni**.
2. Nella finestra visualizzata, selezionare la sezione **Avanzate**.
3. Nella sezione **Certificati**, selezionare la scheda **Protezione** e cliccare sul pulsante **Gestione certificati**.
4. Nella finestra visualizzata, selezionare la scheda **Centri certificati** e cliccare sul pulsante **Ripristina**.
5. Nella finestra visualizzata, selezionare il file di certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Nella finestra visualizzata, selezionare le caselle relative alle azioni da convalidare con il certificato installato. Per visualizzare le informazioni relative al certificato, cliccare sul pulsante **Visualizza**.

➡ *Per installare il certificato di Kaspersky Lab per Mozilla Firefox versione 3.?, eseguire le operazioni seguenti:*

1. Nel menu del browser, selezionare la voce **Strumenti** → **Opzioni**.
2. Nella finestra visualizzata, selezionare la sezione **Avanzate**.
3. Nella scheda **Crittografia**, cliccare sul pulsante **Visualizzazione certificati**.
4. Nella finestra visualizzata, selezionare la scheda **Centri certificati** e cliccare sul pulsante **Importa**.
5. Nella finestra visualizzata, selezionare il file di certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente: *%AllUsersProfile%\Application Data\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.
6. Nella finestra visualizzata, selezionare le caselle relative alle azioni da convalidare con il certificato installato. Per visualizzare le informazioni relative al certificato, cliccare sul pulsante **Visualizza**.

Se il computer viene eseguito con il sistema operativo Microsoft Windows Vista, il percorso del file di certificato di Kaspersky Lab è il seguente: *%AllUsersProfile%\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer*.

SCANSIONE DELLE CONNESSIONI CRITTOGRAFATE IN OPERA

Il browser Opera non utilizza la memoria certificati di Microsoft Windows. Per eseguire la scansione delle connessioni SSL in Opera, è necessario installare il certificato di Kaspersky Lab manualmente.

➡ *Per installare il certificato di Kaspersky Lab, eseguire le operazioni seguenti:*

1. Nel menu del browser, selezionare la voce **Strumenti** → **Preferenze**.
2. Nella finestra visualizzata, selezionare la sezione **Avanzate**.
3. Nella parte sinistra della finestra, selezionare la scheda **Protezione** e cliccare sul pulsante **Gestisci certificati**.

4. Nella finestra visualizzata, selezionare la scheda **Fornitori** e cliccare sul pulsante **Importa**.

5. Nella finestra visualizzata, selezionare il file di certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
   %AllUsersProfile%\Application Data\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. Nella finestra visualizzata, cliccare sul pulsante **Installa**. Il certificato di Kaspersky Lab verrà installato. Per visualizzare le informazioni sul certificato e selezionare le azioni per le quali il certificato verrà utilizzato, selezionare il certificato nell'elenco e premere il pulsante **Visualizza**.

Per installare il certificato di Kaspersky Lab per Opera versione 9.x, eseguire le operazioni seguenti:

1. Nel menu del browser, selezionare la voce **Strumenti** → **Preferenze**.

2. Nella finestra visualizzata, selezionare la sezione **Avanzate**.

3. Nella parte sinistra della finestra, selezionare la scheda **Protezione** e cliccare sul pulsante **Gestisci certificati**.

4. Nella finestra visualizzata, selezionare la scheda **Centri certificati** e cliccare sul pulsante **Importa**.

5. Nella finestra visualizzata, selezionare il file di certificato di Kaspersky Lab. Il percorso del file di certificato di Kaspersky Lab è il seguente:
   %AllUsersProfile%\Application Data\Kaspersky Lab\AVP8\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.

6. Nella finestra visualizzata, cliccare sul pulsante **Installa**. Il certificato di Kaspersky Lab verrà installato.

DISCO DI RIPRISTINO

Kaspersky Anti-Virus comprende un servizio che consente di creare un Disco di Ripristino.

Disco di Ripristino è stato progettato per eseguire la scansione dei computer compatibili con le piattaforme x86 e per disinfettarli. È consigliabile utilizzarlo quando il livello di infezione è tale da reputare impossibile la disinfezione tramite applicazioni anti-virus o utilità di rimozione di malware, ad esempio Kaspersky AVPTool, del sistema operativo. In questo caso, è possibile ottenere un livello di efficacia della disinfezione superiore, in quanto i programmi malware non ottengono il controllo quando viene caricato il sistema operativo.

Disco di Ripristino è un file con estensione iso basato sulla piattaforma Linux che include gli elementi seguenti:

- file di sistema e file Linux di configurazione;
- una serie di utilità diagnostiche per il sistema operativo;
- una serie di strumenti aggiuntivi (gestione file e così via);
- file di Disco di Ripristino Kaspersky;
- file contenenti i database dell'applicazione.

È possibile avviare un computer con un sistema operativo danneggiato in uno dei due modi seguenti:

- *in locale*, da un CD/DVD. A tale scopo, è necessario che il computer sia dotato di un dispositivo appropriato.
- *in remoto*, dalla stazione di lavoro dell'amministratore o da un altro computer sulla rete.

> È possibile eseguire l'avvio remoto solo se il computer da avviare supporta la tecnologia Intel® vPro™ o Intel® Active Management.

Per creare un Disco di Ripristino, eseguire le seguenti operazioni:

1. Aprire la finestra principale dell'applicazione.
2. Cliccare sul pulsante **Disco di Ripristino** per eseguire la creazione guidata del Disco di Ripristino (vedere pagina 176).
3. Seguire le istruzioni della procedura guidata.
4. Utilizzando il file fornito con la procedura guidata, creare un CD/DVD di avvio. A tale scopo, è possibile utilizzare un'applicazione di masterizzazione di CD/DVD, come Nero.

VEDERE ANCHE

Creazione del Disco di Ripristino....................176

Avvio del computer attraverso il Disco di Ripristino....................178

CREAZIONE DEL DISCO DI RIPRISTINO

La creazione del Disco di Ripristino comporta la creazione di un'immagine del disco (file ISO) con database e file di configurazione anti-virus aggiornati.

L'immagine del disco di origine da utilizzare come base per la creazione del nuovo file può essere scaricata dal server Kaspersky Lab o copiata da un'origine locale.

Il file di immagine creato mediante la procedura guidata verrà salvato nella cartella "*Documents and Settings\All Users\Dati applicazioni\Kaspersky Lab\AVP80\Data\Rdisk*" o "*ProgramData\Kaspersky Lab\AVP80\Data\Rdisk*" per Microsoft Vista e verrà denominato *rescuecd.iso*. Se la procedura guidata rileva un file ISO creato in precedenza nella cartella specificata, è possibile utilizzarlo come immagine del disco originale selezionando la casella **Usa file ISO esistente** e andare al passaggio 3 in cui viene eseguito l'aggiornamento dell'immagine (vedere pagina 177). Se la procedura guidata non rileva alcun file di immagine, questa casella non sarà disponibile.

Il Disco di Ripristino viene creato con una procedura guidata composta da una serie di caselle (passaggi). È possibile selezionare le diverse caselle con i bottoni **Indietro** e **Avanti**; per completare la procedura guidata, cliccare sul pulsante **Fine**. Per interrompere la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

DESCRIZIONE DETTAGLIATA DEI PASSAGGI DELLA PROCEDURA GUIDATA

Passaggio 1. Selezione dell'origine dell'immagine del Disco di emergenza 177

Passaggio 2. Copia dell'immagine ISO 177

Passaggio 3. Aggiornamento dell'immagine ISO 177

Passaggio 4. Avvio remoto 178

Passaggio 5. Chiusura della procedura guidata 178

PASSAGGIO 1. SELEZIONE DELL'ORIGINE DELL'IMMAGINE DEL DISCO DI EMERGENZA

Se è stata selezionata la casella **Usa file ISO esistente** nella finestra della procedura guidata precedente, questo passaggio verrà ignorato.

Durante questo passaggio, è necessario selezionare l'origine del file di immagine nell'elenco di opzioni:

- Selezionare **Copiare l'immagine ISO da un CD/DVD o dalla rete locale** se si dispone già di un Disco di Ripristino su CD/DVD o di un'immagine preparata per il disco e memorizzata nel computer o in una risorsa di rete locale.
- Selezionare l'opzione **Scaricare l'immagine ISO dal server Kaspersky Lab** se non si dispone di un file di immagine esistente. Questa opzione consente di scaricare il file dal server Kaspersky Lab (la dimensione del file è di circa 100 MB).

PASSAGGIO 2. COPIA DELL'IMMAGINE ISO

Se nel passaggio precedente è stata selezionata l'opzione di copia dell'immagine da un'origine locale, ovvero **Copiare l'immagine ISO dal CD/DVD o dalla rete locale**, è necessario specificare il percorso dell'immagine nel passaggio corrente. A questo scopo, utilizzare il pulsante **Sfoglia**. Verrà quindi visualizzato lo stato di avanzamento della copia.

Se è stata selezionata l'opzione **Scaricare l'immagine ISO dal server Kaspersky Lab**, lo stato di avanzamento del download del file verrà visualizzato immediatamente.

PASSAGGIO 3. AGGIORNAMENTO DELL'IMMAGINE ISO

La procedura di aggiornamento dei file include:

- aggiornamento dei database dell'applicazione;
- aggiornamento dei file di configurazione.

I file di configurazione determinano le modalità di utilizzo del Disco di Ripristino: su un computer locale o remoto; pertanto, è necessario selezionare un'opzione prima di aggiornare il file ISO:

- **Avvio remoto** se si intende caricare un computer remoto.

  Se è selezionato l'avvio di un computer remoto, questo deve supportare la tecnologia Intel® vPro™ o Intel® Active Management.

  Se l'accesso a Internet da un computer remoto viene garantito da un proxy, non sarà possibile eseguire l'aggiornamento mediante il Disco di Ripristino. In tal caso, si consiglia di aggiornare prima Kaspersky Anti-Virus.

- **Avvio dal disco CD/DVD** se l'immagine del disco creata è destinata ad essere registrata su un CD/DVD.

Una volta selezionata l'opzione, cliccare sul pulsante **Avanti**. Nella finestra successiva della procedura guidata verrà visualizzato lo stato di avanzamento dell'aggiornamento.

Se è stata selezionata l'opzione **Avvio remoto**, non sarà possibile utilizzare l'immagine creata né per masterizzare un CD/DVD, né per caricare il computer. Per caricare il computer da un CD/DVD, è necessario avviare di nuovo la procedura guidata e selezionare l'opzione **Avvio dal disco CD/DVD** durante questo passaggio.

PASSAGGIO 4. AVVIO REMOTO

Questo passaggio della procedura guidata viene visualizzato solo se è stata selezionata l'opzione **Avvio remoto** durante il passaggio precedente.

Immettere le informazioni sul computer:

- **Indirizzo IP o nome computer** sulla rete;
- I dati dell'account utente con diritti di amministratore del sistema: **Nome utente** e **Password**.

La finestra successiva della procedura guidata è una console iAMT in cui è possibile controllare il processo di caricamento del computer (vedere pagina 178).

PASSAGGIO 5. CHIUSURA DELLA PROCEDURA GUIDATA

In questa finestra della procedura guidata viene visualizzato un messaggio che indica che un Disco di Ripristino è stato creato correttamente.

AVVIO DEL COMPUTER ATTRAVERSO IL DISCO DI RIPRISTINO

Se non è possibile eseguire l'avvio del sistema operativo a causa dell'attacco di un virus, utilizzare il Disco di Ripristino.

Per caricare il sistema operativo, sarà necessario il file di immagine del disco di avvio (con estensione iso). È possibile scaricare (vedere pagina 177) il file da un server di Kaspersky Lab oppure aggiornare (vedere pagina 177) quello esistente.

Di seguito viene illustrato in modo dettagliato il funzionamento del Disco di Ripristino. Durante il caricamento del disco, vengono eseguite le operazioni seguenti:

1. Rilevamento automatico dell'hardware del computer.

2. Ricerca dei file system nei dischi rigidi. Ai file system rilevati verranno assegnati nomi che iniziano con "*C*.

   È possibile che ai dischi rigidi e ai dispositivi rimovibili vengano assegnati nomi che non corrispondono a quelli assegnati dal sistema operativo.

   Se il sistema operativo del computer caricato è in modalità di sospensione o se il relativo file system presenta lo stato *infetto* a causa di una chiusura non corretta, l'utente potrà scegliere se installare il file system o riavviare il computer.

   L'installazione del file system potrebbe comportarne il danneggiamento.

3. Ricerca del file swap di Microsoft Windows *pagefile.sys*. Se tale file è assente, il volume della memoria virtuale sarà limitato dalla dimensione della RAM.

4. Selezione della lingua di localizzazione. Se la selezione non viene effettuata dopo un determinato intervallo di tempo, per impostazione predefinita verrà impostata la lingua inglese.

   Quando si carica un computer remoto, tale passaggio viene ignorato.

5. Ricerca (creazione) nelle cartelle di database anti-virus, rapporti, memoria di quarantena e file aggiuntivi. Per impostazione predefinita, verranno utilizzate le cartelle dell'applicazione di Kaspersky Lab, installate nel computer infetto (*ProgramData/Kaspersky Lab/AVP8* – per Microsoft Windows Vista, *Documents and Settings/All Users/Dati applicazioni/Kaspersky Lab/AVP8* – per le versioni precedenti di Microsoft Windows). Se non è possibile individuare tali cartelle, verrà effettuato il tentativo di crearle. Se non è possibile trovare le cartelle né crearle, la cartella *kl.files* verrà creata in un disco di sistema.

6. Tentativo di configurazione delle connessioni di rete in base ai dati rilevati nei system file del computer di cui è in corso il caricamento.

7. Caricamento di un sottosistema grafico e avvio del Disco di Ripristino di Kaspersky (in caso di caricamento del computer da un CD/DVD).

   Se un computer remoto viene caricato nella console iAMT, verrà caricato il prompt dei comandi. È possibile utilizzare i comandi per l'utilizzo del Disco di Ripristino di Kaspersky dalla riga di comando per gestire le attività (vedere pagina 181).

Nella modalità di ripristino del sistema sono disponibili solo le attività di scansione anti-virus e di aggiornamento dei database da un'origine locale, nonché il rollback degli aggiornamenti e la visualizzazione delle statistiche.

➡ *Per caricare il sistema operativo di un computer infetto da un CD/DVD, eseguire le seguenti operazioni:*

1. Nelle impostazioni del BIOS abilitare l'avvio dal CD/DVD-ROM. Per informazioni dettagliate, fare riferimento alla documentazione relativa alla scheda madre installata nel computer.

2. Inserire il CD/DVD con l'immagine del Disco di Ripristino nell'unità CD/DVD di un computer infetto.

3. Riavviare il computer.

4. Le operazioni di avvio successive verranno eseguite in base all'algoritmo descritto prima.

➡ *Per caricare il sistema operativo di un computer remoto, eseguire le seguenti operazioni:*

1. Aprire la finestra principale dell'applicazione.

2. Cliccare sul pulsante **Disco di Ripristino** per eseguire la creazione guidata del Disco di Ripristino (vedere pagina 176). Seguire le istruzioni della procedura guidata.

È necessario selezionare l'opzione **Avvio remoto** durante la fase di aggiornamento dell'immagine del disco (vedere pagina 177).

Le operazioni di avvio successive verranno eseguite in base all'algoritmo descritto prima.

UTILIZZO DEL DISCO DI RIPRISTINO DI KASPERSKY DAL PROMPT DEI COMANDI

È possibile utilizzare il Disco di Ripristino di Kaspersky dal prompt dei comandi. In tal caso sono consentite le operazioni seguenti:

- scansione di oggetti selezionati;
- aggiornamento dei database e dei moduli dell'applicazione;
- rollback dell'ultimo aggiornamento;
- richiamo della Guida nella sintassi della riga di comando;
- richiamo della Guida nella sintassi dei comandi.

Sintassi della riga di comando:

```
<comando> [impostazioni]
```

È possibile utilizzare i seguenti comandi:

HELP	fornisce indicazioni sulla sintassi dei comandi e sull'elenco dei comandi
SCAN	esegue la scansione anti-virus degli oggetti
UPDATE	aggiorna l'avvio dell'attività
ROLLBACK	ultimo rollback di aggiornamento
EXIT	consente di uscire dal Disco di Ripristino di Kaspersky

IN QUESTA SEZIONE

Scansione anti-virus 181

Aggiornamento di Kaspersky Anti-Virus 183

Rollback dell'ultimo aggiornamento 183

Visualizzazione della Guida 184

SCANSIONE ANTI-VIRUS

L'avvio della scansione anti-virus di una determinata area e l'elaborazione degli oggetti dannosi dalla riga di comando generalmente presenta la sintassi seguente:

```
SCAN [<oggetto esaminato>] [<azione>] [<tipi di file>] [<esclusioni>] [<impostazioni
rapporto>]
```

Descrizione delle impostazioni:

<oggetto esaminato>: questo parametro fornisce l'elenco di oggetti che verranno esaminati per rilevare eventuale codice dannoso. Può includere diversi valori dell'elenco fornito separati da spazi.	
<file>	Elenco di percorsi dei file e/o delle cartelle da esaminare. È possibile indicare un percorso assoluto o relativo. Gli elementi dell'elenco devono essere separati da uno spazio. Commenti: • Se il nome dell'oggetto contiene uno spazio, esso deve essere incluso tra virgolette. • Se viene fatto riferimento a una directory specifica, verranno esaminati tutti i file in essa contenuti.
/discs/	Scansione di tutte le unità.
/discs/<nome_disco>:/<cartella>	Scansione dell'unità selezionata, in cui <nome_disco> corrisponde al nome dell'unità, mentre <cartella> rappresenta il percorso della cartella da esaminare.
<azione>: questo parametro determina le azioni che verranno eseguite sugli oggetti dannosi rilevati durante la scansione. Se non è definito, l'azione predefinita è quella con il valore **-i8**.	
-i0	Nessuna azione sull'oggetto; solo registrazione delle informazioni nel rapporto.
-i1	Gli oggetti infetti vengono elaborati e, se la disinfezione è impossibile, vengono ignorati.
-i2	Gli oggetti infetti vengono elaborati e, se la disinfezione non riesce, vengono eliminati. Non vengono eliminati gli oggetti infetti appartenenti a oggetti compositi. Per impostazione predefinita, vengono eliminati gli oggetti composti con intestazione eseguibile (archivi .sfx).
-i3	Gli oggetti infetti vengono elaborati e, se la disinfezione non riesce, vengono eliminati. Vengono eliminati tutti gli oggetti composti se non è possibile eliminare le parti infette.
-i4	Vengono eliminati gli oggetti infetti. Vengono eliminati tutti gli oggetti composti se non è possibile eliminare le parti infette.
-i8	Viene richiesto l'intervento dell'utente se viene rilevato un oggetto infetto.
-i9	Viene richiesto l'intervento dell'utente al termine della scansione.
<tipi file>: questo parametro definisce i tipi di file che saranno sottoposti alla scansione anti-virus. Per impostazione predefinita, questo parametro non è specificato e sono sottoposti a scansione solo i file infetti in base al contenuto.	
-fe	Vengono esaminati solo i file infetti in base all'estensione.
-fi	Vengono esaminati solo i file infetti in base al contenuto.
-fa	Vengono esaminati tutti i file.
<esclusioni>: questo parametro definisce gli oggetti esclusi dalla scansione. Può includere diversi valori dell'elenco fornito separati da spazi.	

-e:a	Non vengono esaminati gli archivi.
-e:b	Non vengono esaminati i database della posta.
-e:m	Non vengono esaminati i messaggi di posta con testo semplice.
-e:<mascherafile>	Non vengono esaminati gli oggetti corrispondenti alla maschera.
-e:<secondi>	Vengono ignorati gli oggetti la cui scansione richiede un intervallo di tempo superiore a quello specificato nel parametro **<secondi>**.
-es:<dimensione>	Vengono ignorati gli oggetti di dimensioni (in MB) superiori a quelle specificate nel parametro **<dimensione>**.

Esempi:

- *Avvio della scansione della cartella Documents and Settings e dell'unità <D>:*

```
SCAN /discs/D: "/discs/C:/Documents and Settings"
```

AGGIORNAMENTO DI KASPERSKY ANTI-VIRUS

La sintassi del comando per l'aggiornamento dei database e dei moduli del programma di Kaspersky Anti-Virus è la seguente:

```
UPDATE [<origine_aggiornamenti>] [-R[A]:<file_rapporto>]
```

Descrizione delle impostazioni:

<sorgente_aggiornamenti>	Server HTTP o FTP o cartella di rete per il download degli aggiornamenti. Il valore dell'impostazione può essere nel formato di un percorso completo di un URL o di un'origine degli aggiornamenti. Se non si seleziona il percorso, l'origine degli aggiornamenti verrà desunta dalle impostazioni del servizio di aggiornamento di Kaspersky Anti-Virus.
-/R[A]:<file_rapporti>	**-R:<file_rapporti>**: registra solo eventi importanti nel rapporto. **-RA:<file_rapporti>**: registra tutti gli eventi nel rapporto. È possibile utilizzare un percorso assoluto al file. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.

Esempi:

- *Aggiornamento dei database e registrazione di tutti gli eventi in un rapporto:*

```
UPDATE -RA:/discs/C:/avbases_upd.txt
```

ROLLBACK DELL'ULTIMO AGGIORNAMENTO

Sintassi del comando:

```
ROLLBACK [-R[A]:<file_rapporti>]
```

Descrizione delle impostazioni:

-/R[A]:<file_rapporti>	**-R:<file_rapporti>**: registra solo eventi importanti nel rapporto. **-RA:<file_rapporti>**: registra tutti gli eventi nel rapporto. È possibile utilizzare un percorso assoluto al file. Se il parametro non è

	definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.

Esempio:

```
ROLLBACK -RA:/discs/C:/rollback.txt
```

VISUALIZZAZIONE DELLA GUIDA

Questo comando consente di visualizzare la sintassi della riga di comando dell'applicazione:

```
[ -? | HELP ]
```

Per visualizzare la Guida per la sintassi di un comando specifico, è possibile utilizzare uno dei comandi seguenti:

```
<comando> -?
HELP <comando>
```

VERIFICA DEL FUNZIONAMENTO DI KASPERSKY ANTI-VIRUS

Dopo aver installato e configurato Kaspersky Anti-Virus, è possibile verificare la correttezza della configurazione tramite un virus di "prova" e le sue varianti. Per ciascun protocollo / componente di protezione è necessario eseguire un test separato.

IN QUESTA SEZIONE

"Virus" di prova EICAR e sue varianti 185

Test della protezione del traffico HTTP 186

Test della protezione del traffico SMTP 187

Verifica del funzionamento di Anti-Virus File 187

Verifica del funzionamento dell'attività di scansione anti-virus 187

Verifica del funzionamento di Anti-Spam 188

"VIRUS" DI PROVA EICAR E SUE VARIANTI

Questo "virus" di prova è stato progettato specificamente da eicar (European Institute for Computer Antivirus Research) per il collaudo dei prodotti anti-virus.

Il "virus" di prova NON È UN VIRUS, poiché non contiene codice in grado di danneggiare il computer. Tuttavia, la maggior parte dei prodotti anti-virus lo identifica come tale.

Si raccomanda di non utilizzare mai virus autentici per verificare il corretto funzionamento di un programma anti-virus.

È possibile scaricare il "virus" di prova dal sito Web ufficiale di **EICAR** all'indirizzo http://www.eicar.org/anti_virus_test_file.htm.

Prima di scaricare il file, è necessario disabilitare la protezione anti-virus del computer perché altrimenti l'applicazione identificherà ed elaborerà il file *anti_virus_test_file.htm* come oggetto infetto trasferito tramite il protocollo HTTP. Riattivare la protezione anti-virus subito dopo aver scaricato il "virus" di prova.

L'applicazione identifica il file scaricato dal sito **EICAR** come oggetto infetto contenente un virus che **impossibile disinfettare** ed esegue le azioni specificate per questo tipo di oggetto.

È possibile inoltre utilizzare varianti del "virus" di prova standard per verificare il funzionamento dell'applicazione. A tal fine, modificare il contenuto del "virus" standard aggiungendo uno dei prefissi elencati nella tabella di seguito. Per modificare il "virus" di prova, è possibile utilizzare qualsiasi editor di testo o di ipertesto, ad esempio **Blocco note Microsoft**, **UltraEdit32** e così via.

È possibile verificare il corretto funzionamento dell'applicazione anti-virus tramite il "virus" modificato EICAR solo se i database anti-virus sono aggiornati almeno al 24 ottobre 2003 (Ottobre 2003, aggiornamenti cumulativi).

Nella tabella seguente la prima colonna contiene i prefissi che devono essere aggiunti all'inizio della stringa del "virus" di prova standard. La seconda colonna elenca tutti i valori possibili dello stato che l'applicazione Anti-Virus può assegnare

all'oggetto in base ai risultati della scansione. La terza colonna indica come vengono elaborati gli oggetti che presentano lo stato specificato. Si noti che le azioni eseguite sugli oggetti sono determinate dalle impostazioni dell'applicazione.

Dopo aver aggiunto un prefisso al "virus" di prova, salvare il nuovo file con un nome diverso, ad esempio:*eicar_dele.com*. Assegnare nomi simili a tutti i "virus" modificati.

Table 1. Varianti del "virus" di prova

Prefisso	Stato dell'oggetto	Informazioni di elaborazione dell'oggetto
Nessun prefisso, "virus" di prova standard.	**Infetto**. L'oggetto contiene codice di un virus noto e non può essere disinfettato.	L'applicazione identifica l'oggetto come virus non disinfettabile. Si verifica un errore nel tentativo di disinfettare l'oggetto; verrà eseguita l'azione specificata per gli oggetti non disinfettabili.
CORR–	**Oggetti danneggiati**.	L'applicazione ha potuto accedere all'oggetto ma non ha potuto esaminarlo, poiché l'oggetto è danneggiato, ad esempio la struttura del file è danneggiata o il formato file non è valido. Informazioni sull'elaborazione dell'oggetto sono disponibili nel rapporto sul funzionamento dell'applicazione.
WARN–	**Sospetto**. L'oggetto contiene codice di un virus sconosciuto e non può essere disinfettato.	L'oggetto è stato ritenuto sospetto dall'analizzatore euristico di codice. Al momento del rilevamento, i database delle firme delle minacce dell'Anti-Virus non contengono alcuna descrizione della procedura per il trattamento di questo oggetto. Il rilevamento di un oggetto di questo tipo viene notificato.
SUSP–	**Sospetto**. L'oggetto contiene codice modificato di un virus noto e non può essere disinfettato.	L'applicazione ha rilevato una corrispondenza parziale tra una sezione di codice dell'oggetto e una sezione di codice di un virus noto. Al momento del rilevamento, i database delle firme delle minacce dell'Anti-Virus non contengono alcuna descrizione della procedura per il trattamento di questo oggetto. Il rilevamento di un oggetto di questo tipo viene notificato.
ERRO–	**Errore di scansione**.	Si è verificato un errore durante la scansione di un oggetto. L'applicazione non ha potuto eseguire l'accesso all'oggetto, in quanto l'integrità dell'oggetto è stata compromessa, ad esempio a causa di un archivio in più volumi, o non è stata stabilita una connessione a esso, ad esempio se l'oggetto viene esaminato in una risorsa di rete. Informazioni sull'elaborazione dell'oggetto sono disponibili nel rapporto sul funzionamento dell'applicazione.
CURE–	**Infetto**. L'oggetto contiene codice di un virus noto disinfettato.	L'oggetto contiene un virus che può essere disinfettato. L'applicazione disinfetterà l'oggetto; il testo del corpo del "virus" verrà sostituito dalla parola CURE. Il rilevamento di un oggetto di questo tipo viene notificato.
DELE–	**Infetto**. L'oggetto contiene codice di un virus noto e non può essere disinfettato.	L'applicazione identifica l'oggetto come virus non disinfettabile. Si verifica un errore nel tentativo di disinfettare l'oggetto; verrà eseguita l'azione specificata per gli oggetti non disinfettabili. Il rilevamento di un oggetto di questo tipo viene notificato.

TEST DELLA PROTEZIONE DEL TRAFFICO HTTP

➡ *Per verificare che i virus siano stati rilevati correttamente nel flusso di dati trasferito attraverso il protocollo HTTP, eseguire le operazioni seguenti:*

TProvare a scaricare il "virus" di prova dal sito Web ufficiale di **EICAR** all'indirizzo http://www.eicar.org/anti_virus_test_file.htm.

Quando il computer tenta di scaricare il "virus" di prova, Kaspersky Anti-Virus rileva questo oggetto identificandolo come oggetto infetto non disinfettabile, ed esegue l'azione specificata nelle impostazioni di scansione del traffico HTTP per gli oggetti che presentano questo stato. Per impostazione predefinita, quando si tenta di scaricare il "virus" di prova, la

connessione al sito Web viene terminata e nel browser viene visualizzato un messaggio che informa l'utente che l'oggetto è stato infettato dal virus EICAR-Test-File.

TEST DELLA PROTEZIONE DEL TRAFFICO SMTP

Per rilevare i virus presenti nei flussi di dati trasferiti tramite il protocollo SMTP, è necessario utilizzare un sistema di posta elettronica che utilizzi questo protocollo per trasferire i dati.

Si consiglia di verificare la modalità con cui l'Anti-Virus gestisce i messaggi di posta elettronica in uscita, inclusi il corpo del messaggio e gli allegati. Per testare la funzione di rilevamento dei virus nel corpo del messaggio, copiare il testo del "virus" di prova standard o di quello modificato nel corpo del messaggio.

A tale scopo:

1. Creare un messaggio nel formato di **testo normale** utilizzando il client di posta installato nel computer.

   Se creato in formato RTF o HTML, il messaggio contenente il virus di prova non verrà esaminato.

2. Copiare il testo del "virus" standard o modificato all'inizio del messaggio o allegare al messaggio un file contenente il "virus" di prova.

3. Inviare il messaggio all'amministratore.

L'applicazione individuerà l'oggetto, lo identificherà come infetto e lo bloccherà.

VERIFICA DEL FUNZIONAMENTO DI ANTI-VIRUS FILE

Per verificare che Anti-Virus File sia configurato correttamente, eseguire le seguenti operazioni:

1. Creare una cartella su disco. Copiare nella cartella il "virus" di prova scaricato dal sito Web ufficiale di **EICAR** (http://www.eicar.org/anti_virus_test_file.htm), nonché tutte le varianti create.

2. Lasciare che tutti gli eventi vengano registrati, in modo che il file del rapporto conservi i dati sugli oggetti danneggiati o su quelli non esaminati a causa di errori.

3. Eseguire il virus "di prova" o una delle relative versioni modificate.

Anti-Virus File intercetta il tentativo di eseguire il file, lo esamina ed esegue l'azione specificata nelle impostazioni per gli oggetti che presentano quello stato. Selezionando diverse azioni da eseguire sull'oggetto rilevato, è possibile effettuare un controllo completo del funzionamento del componente.

Il rapporto sul funzionamento del componente include informazioni sui risultati dell'operazione eseguita da Anti-Virus File.

VERIFICA DEL FUNZIONAMENTO DELL'ATTIVITÀ DI SCANSIONE ANTI-VIRUS

Per verificare che l'attività di scansione anti-virus funzioni correttamente:

1. Creare una cartella su disco. Copiare nella cartella il "virus" di prova scaricato dal sito Web ufficiale di **EICAR** (http://www.eicar.org/anti_virus_test_file.htm), nonché tutte le varianti create.

2. Creare una nuova attività di scansione anti-virus e selezionare la cartella contenente il gruppo di "virus" di prova come oggetto da esaminare.

3. Lasciare che tutti gli eventi vengano registrati, in modo che il file del rapporto conservi i dati sugli oggetti danneggiati e su quelli non esaminati a causa di errori.

4. Eseguire l'attività di scansione anti-virus.

Quando l'attività di scansione è in esecuzione, le azioni specificate nelle impostazioni verranno eseguite al rilevamento di oggetti infetti o sospetti. Selezionando diverse azioni da eseguire sull'oggetto rilevato, è possibile effettuare un controllo completo del funzionamento del componente.

È possibile visualizzare tutte le informazioni sulle azioni dell'attività di scansione anti-virus nel rapporto sul funzionamento del componente.

VERIFICA DEL FUNZIONAMENTO DI ANTI-SPAM

È possibile utilizzare un messaggio di prova identificato come SPAM per testare la protezione Anti-Spam.

Il corpo del messaggio di prova deve contenere la seguente riga:

```
Spam is bad do not send it
```

Un volta ricevuto questo messaggio nel computer, Kaspersky Anti-Virus lo esamina e gli assegna lo stato di spam ed esegue l'azione specificata per gli oggetti di questo tipo.

TIPI DI NOTIFICHE

Quando si verificano eventi di Kaspersky Anti-Virus, vengono visualizzati messaggi di notifica speciali. A seconda della criticità dell'evento per la protezione del computer, potrebbero essere visualizzati i tipi di notifica seguenti:

- **Allarme**. Si è verificato un evento critico, ad esempio è stato rilevato un oggetto dannoso o un'attività pericolosa nel sistema. È necessario decidere subito come affrontare la minaccia. Questo tipo di notifica è visualizzata in rosso.
- **Attenzione**. Si è verificato un evento potenzialmente pericoloso. Ad esempio, nel sistema sono stati rilevati file potenzialmente infetti o un'attività sospetta. È necessario stabilire quanto è pericoloso l'evento in questione. Questo tipo di notifica è visualizzata in giallo.
- **Informazioni**. Questa notifica fornisce informazioni su eventi non critici. Questo tipo di notifica include, tra l'altro, le notifiche che vengono visualizzate durante la apprendimento di Anti-Hacker. Le notifiche informative sono visualizzate in blu.

IN QUESTA SEZIONE

Rilevamento di un oggetto dannoso 189

Impossibile disinfettare l'oggetto 190

Richiesta di esecuzione di una procedura speciale 191

Rilevamento di un oggetto sospetto 191

Rilevamento di un oggetto pericoloso nel traffico 192

Rilevamento di un'attività pericolosa nel sistema 192

Rilevamento di un intruso 193

Rilevamento di processi nascosti 193

Rilevamento di un tentativo di accesso al Registro di sistema 194

Rilevamento di un tentativo di reindirizzamento delle chiamate alle funzioni di sistema 194

Rilevamento dell'attività di rete di un'applicazione 195

Rilevamento dell'attività di rete di un file eseguibile modificato 196

Rilevamento di una nuova rete 196

Rilevamento di un attacco di phishing 196

Rilevamento di un tentativo di composizione automatica 197

Rilevamento di un certificato non valido 197

RILEVAMENTO DI UN OGGETTO DANNOSO

Se Anti-Virus File, Anti-Virus Posta o una scansione anti-virus rileva un codice dannoso, viene visualizzata una notifica speciale.

Tale notifica indica:

- Il tipo di minaccia, ad esempio *virus*, *Trojan*, e il nome dell'oggetto dannoso così come è elencato nella Virus Encyclopedia di Kaspersky Lab. Il nome dell'oggetto pericoloso viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata nel computer.
- Il nome completo dell'oggetto dannoso e il relativo percorso.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Disinfetta**: viene eseguito un tentativo di disinfezione dell'oggetto dannoso. Prima del trattamento, viene eseguita una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.
- **Elimina**: l'oggetto dannoso viene eliminato. Prima dell'eliminazione, viene creata una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.
- **Salta**: l'accesso all'oggetto viene bloccato e non viene eseguita alcuna azione su di esso. Verranno semplicemente registrate informazioni sull'oggetto in un rapporto.

  Successivamente sarà possibile tornare agli oggetti dannosi ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o dell'attività di protezione, selezionare la casella ☑ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

IMPOSSIBILE DISINFETTARE L'OGGETTO

In alcuni casi può risultare impossibile disinfettare un oggetto dannoso. Questo può succedere se un file è talmente danneggiato che diventa impossibile eliminarne il codice dannoso e ripristinarne l'integrità. La procedura di disinfezione di questi casi non può essere eseguita su diversi tipi di oggetti pericolosi, ad esempio i Trojan.

In queste situazioni verrà visualizzata una notifica speciale con le informazioni seguenti:

- Il tipo di minaccia, ad esempio *virus*, *Trojan*, e il nome dell'oggetto dannoso così come è elencato nella Virus Encyclopedia di Kaspersky Lab. Il nome dell'oggetto pericoloso viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata nel computer.
- Il nome completo dell'oggetto dannoso e il relativo percorso.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Elimina**: l'oggetto dannoso viene eliminato. Prima dell'eliminazione, viene creata una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.
- **Salta**: l'accesso all'oggetto viene bloccato e non viene eseguita alcuna azione su di esso. Verranno semplicemente registrate informazioni sull'oggetto in un rapporto.

  Successivamente sarà possibile tornare agli oggetti dannosi ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o dell'attività di protezione, selezionare la casella ☑ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla relativa disabilitazione o al relativo riavvio o all'intervallo di tempo dall'inizio di un'attività di scansione anti-virus fino al relativo completamento.

RICHIESTA DI ESECUZIONE DI UNA PROCEDURA SPECIALE

Quando viene rilevata una minaccia attualmente attiva nel sistema, ad esempio un processo dannoso nella RAM o negli oggetti di avvio, viene visualizzato un messaggio per richiedere l'esecuzione di una speciale procedura avanzata di disinfezione.

Gli specialisti di Kaspersky Lab consigliano di accettare l'esecuzione di tale procedura avanzata. A tale scopo, premere il pulsante **OK**. Tenere presente, tuttavia, che il computer verrà riavviato al termine della procedura e pertanto si consiglia di salvare il lavoro corrente e chiudere tutte le applicazioni prima di eseguire la procedura.

Durante l'esecuzione della procedura di disinfezione, non è possibile avviare sessioni di modifica del Registro del sistema operativo o del client di posta. Dopo aver riavviato il computer, si consiglia di eseguire una scansione anti-virus completa.

RILEVAMENTO DI UN OGGETTO SOSPETTO

Se Anti-Virus File, Anti-Virus Posta o una scansione anti-virus rilevano un oggetto contenente il codice di un virus sconosciuto o il codice modificato di un virus noto, viene visualizzata una notifica speciale.

Tale notifica indica:

- Il tipo di minaccia, ad esempio *virus*, *Trojan*, e il nome dell'oggetto così come è elencato nella Virus Encyclopedia di Kaspersky Lab. Il nome dell'oggetto pericoloso viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata nel computer.
- Il nome completo dell'oggetto e il relativo percorso.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Quarantena**: l'oggetto viene messo in quarantena. Quando un oggetto viene messo in Quarantena, viene spostato, non copiato. Esso viene eliminato dal disco o dalla posta elettronica e salvato nella cartella Quarantena. I file in Quarantena vengono salvati in un formato speciale e non sono pericolosi.

  Successivamente, quando si esegue la scansione della cartella Quarantena con firme delle minacce aggiornate, lo stato dell'oggetto potrebbe cambiare. L'oggetto può ad esempio essere identificato come infetto ed essere elaborato utilizzando un database aggiornato. In caso contrario, è possibile assegnare all'oggetto lo stato *non infetto* e quindi ripristinarlo.

  Se un file viene messo in Quarantena manualmente e dopo una successiva scansione risulta non infetto, lo stato non passerà a *OK* immediatamente dopo la scansione. Questo si verificherà solo se la scansione è stata eseguita dopo un determinato intervallo di tempo (almeno tre giorni) in seguito alla messa in quarantena del file.

- **Elimina**: l'oggetto viene eliminato. Prima dell'eliminazione, viene creata una copia di backup dell'oggetto che potrebbe risultare utile per ripristinare l'oggetto o una descrizione della sua infezione.
- **Salta**: l'accesso all'oggetto viene bloccato e non viene eseguita alcuna azione su di esso. Verranno semplicemente registrate informazioni sull'oggetto in un rapporto.

  Successivamente sarà possibile tornare agli oggetti ignorati nella finestra del rapporto. Non sarà tuttavia possibile rimandare l'elaborazione degli oggetti rilevati nei messaggi di posta elettronica.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o dell'attività di protezione, selezionare la casella ☑ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

Se si è certi che l'oggetto rilevato non sia dannoso, si consiglia di aggiungerlo all'area attendibile per evitare che il programma rilevi falsi positivi ripetuti durante l'utilizzo dell'oggetto.

RILEVAMENTO DI UN OGGETTO PERICOLOSO NEL TRAFFICO

Quando Anti-Virus Web rileva un oggetto dannoso nel traffico, viene visualizzata una notifica speciale.

La notifica contiene le informazioni seguenti:

- Il tipo di minaccia, ad esempio *variante virus*, e il nome dell'oggetto pericoloso così come è elencato nella Virus Encyclopedia di Kaspersky Lab. Il nome dell'oggetto viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata.
- Il nome completo dell'oggetto pericoloso con il percorso della pagina Web.

Viene richiesto di selezionare una delle risposte seguenti all'oggetto:

- **Consenti**: il download dell'oggetto continua.
- **Blocca**: il download dell'oggetto dalla risorsa Web viene bloccato.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o dell'attività di protezione, selezionare la casella ☑ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

RILEVAMENTO DI UN'ATTIVITÀ PERICOLOSA NEL SISTEMA

Quando Difesa Proattiva rileva nel sistema un'attività pericolosa dell'applicazione, viene visualizzata una notifica speciale con le informazioni seguenti:

- Il nome della minaccia così come è elencata nella Virus Encyclopedia di Kaspersky Lab. Il nome della minaccia viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata.
- Il nome completo del file del processo che ha avviato l'attività pericolosa e il relativo percorso.
- Risposte possibili:
    - **Quarantena**: il processo viene arrestato e il file eseguibile viene messo in quarantena. Quando un oggetto viene messo in Quarantena, viene solo spostato, non copiato. I file in Quarantena vengono salvati in un formato speciale e non sono pericolosi.

      Successivamente, quando si esegue la scansione della cartella Quarantena con firme delle minacce aggiornate, lo stato dell'oggetto potrebbe cambiare. L'oggetto può ad esempio essere identificato come infetto ed essere elaborato utilizzando un database aggiornato. In caso contrario, è possibile assegnare all'oggetto lo stato *non infetto* e quindi ripristinarlo.

      > Se un file viene messo in Quarantena manualmente e dopo una successiva scansione risulta non infetto, lo stato non passerà a *OK* immediatamente dopo la scansione. Questo si verificherà solo se la scansione è stata eseguita dopo un determinato intervallo di tempo (almeno tre giorni) in seguito alla messa in quarantena del file.

    - **Termina**: arresta il processo.
    - **Consenti**: consente l'esecuzione del processo.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o dell'attività di protezione, selezionare la casella ☑ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di

tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

Se si è certi che il programma rilevato non sia pericoloso, si consiglia di aggiungerlo all'area attendibile per evitare che Kaspersky Anti-Virus generi falsi positivi ripetuti quando lo rileva.

RILEVAMENTO DI UN INTRUSO

Quando Difesa Proattiva rileva un processo che tenta di accedere al sistema, viene visualizzata una notifica speciale con le informazioni seguenti:

- Il nome della minaccia così come è elencata nella Virus Encyclopedia di Kaspersky Lab. Il nome della minaccia viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata.
- Il nome completo del file del processo che ha avviato il tentativo di implementazione e il relativo percorso.
- Risposte possibili:
  - **Termina**: arresta completamente il processo che tenta di accedere.
  - **Blocca**: blocca gli intrusi.
  - **Salta**: non viene eseguita alcuna azione, bensì verranno semplicemente registrate informazioni sul processo in un rapporto.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o di un'attività di protezione, selezionare la casella ☑ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

Se si è certi che l'azione non sia pericolosa, si consiglia di aggiungerla all'area attendibile per evitare che Kaspersky Anti-Virus generi falsi positivi ripetuti quando il processo tenta di accedere a un altro processo.

Ad esempio, se si utilizzano applicazioni che commutano automaticamente le tastiere. Kaspersky Anti-Virus identifica le azioni di tali programmi come pericolose poiché i tentativi di implementazione in altri processi eseguiti da questi programmi sono tipici di vari programmi dannosi (quali gli intercettori delle password).

RILEVAMENTO DI PROCESSI NASCOSTI

Quando Difesa Proattiva rileva nel sistema un'attività nascosta, viene visualizzata una notifica speciale con le informazioni seguenti:

- Il nome della minaccia così come è elencata nella Virus Encyclopedia di Kaspersky Lab. Il nome della minaccia viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata.
- Il nome completo del file del processo nascosto e il relativo percorso.
- Risposte possibili:
  - **Quarantena**: il file eseguibile del processo viene messo in quarantena. Quando un oggetto viene messo in Quarantena, viene solo spostato, non copiato. I file in Quarantena vengono salvati in un formato speciale e non sono pericolosi.

    Successivamente, quando si esegue la scansione della cartella Quarantena con firme delle minacce aggiornate, lo stato dell'oggetto potrebbe cambiare. L'oggetto può ad esempio essere identificato come infetto ed essere elaborato utilizzando un database aggiornato. In caso contrario, è possibile assegnare all'oggetto lo stato *non infetto* e quindi ripristinarlo.

Se un file viene messo in Quarantena manualmente e dopo una successiva scansione risulta non infetto, lo stato non passerà a *OK* immediatamente dopo la scansione. Questo si verificherà solo se la scansione è stata eseguita dopo un determinato intervallo di tempo (almeno tre giorni) in seguito alla messa in quarantena del file.

- **Termina**: arresta il processo.
- **Consenti**: consente l'esecuzione del processo.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o dell'attività di protezione, selezionare la casella ☑ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

Se si è certi che il programma rilevato non sia pericoloso, si consiglia di aggiungerlo all'area attendibile per evitare che Kaspersky Anti-Virus generi falsi positivi ripetuti quando lo rileva.

RILEVAMENTO DI UN TENTATIVO DI ACCESSO AL REGISTRO DI SISTEMA

Quando Difesa Proattiva rileva un tentativo di accesso alle chiavi del Registro di sistema, viene visualizzata una notifica speciale con le informazioni seguenti:

- La chiave del Registro di sistema alla quale si sta tentando di accedere.
- Il nome completo del file del processo che ha avviato il tentativo di accesso alle chiavi del Registro di sistema e il relativo percorso.
- Risposte possibili:
  - **Consenti**: l'esecuzione dell'azione pericolosa viene consentita una volta;
  - **Blocca**: l'azione pericolosa viene bloccata una volta.

Per eseguire l'azione selezionata automaticamente ogni volta che l'attività viene avviata nel computer, selezionare la casella ☑ **Crea una regola**.

Se si è certi che le attività eseguite dall'applicazione che ha tentato di accedere alle chiavi del Registro di sistema non siano pericolose, aggiungere l'applicazione all'elenco di applicazioni attendibili.

RILEVAMENTO DI UN TENTATIVO DI REINDIRIZZAMENTO DELLE CHIAMATE ALLE FUNZIONI DI SISTEMA

Quando Difesa Proattiva rileva un tentativo di incorporate codice nel kernel del sistema operativo Microsoft Windows allo scopo di modificare l'indirizzo per le chiamate alle funzioni di sistema, viene visualizzata una notifica speciale.

Lo scopo della notifica è quello di informare l'utente, in quanto tale comportamento potrebbe essere causato da programmi dannosi nascosti o da un virus sconosciuto nel sistema.

In questa situazione, è consigliabile aggiornare i database dell'applicazione ed eseguire una scansione completa.

RILEVAMENTO DELL'ATTIVITÀ DI RETE DI UN'APPLICAZIONE

Se in Anti-Hacker è attivata la modalità Apprendimento, ogni volta che un'applicazione tenta di stabilire una connessione di rete alla quale con corrisponde alcuna regola, viene visualizzata una notifica speciale sullo schermo.

La notifica contiene le informazioni seguenti:

- *Descrizione dell'attività*: nome dell'applicazione e funzionalità generali della connessione che essa avvia. In genere, vengono specificati il tipo di connessione, la porta locale da cui è stata avviata, la porta remota e l'indirizzo di connessione. Per ottenere informazioni dettagliate sulla connessione, il processo che l'ha avviata e lo sviluppatore dell'applicazione, cliccare sul collegamento **Dettagli**.
- *Azione*: serie di operazioni che il componente Anti-Hacker deve eseguire per l'attività di rete rilevata.

Esaminare attentamente le informazioni relative all'attività di rete e quindi selezionare le azioni da eseguire con Anti-Hacker. È consigliabile utilizzare questi suggerimenti prima di prendere una decisione:

1. Prima di eseguire qualsiasi operazione, decidere se consentire o bloccare l'attività di rete. In questa situazione è possibile che sia stato creato in precedenza un insieme di regole per questa applicazione o pacchetto che possono risultare utili (sempre che sia effettivamente disponibile).
2. Decidere quindi se eseguire l'azione scelta una sola volta o se eseguirla automaticamente ogni volta che l'attività viene rilevata.

Per eseguire l'azione una sola volta,

deselezionare la casella **Crea una regola** e selezionare l'azione richiesta, ovvero **Permetti** o **Blocca**.

Per eseguire automaticamente l'azione selezionata ogni volta che l'attività viene rilevata nel computer, eseguire le seguenti operazioni:

1. Verificare che la casella **Crea una regola** sia selezionata.
2. Selezionare nell'elenco a discesa il tipo di attività a cui deve essere applicata l'azione:
   - **Qualsiasi attività**: qualsiasi attività di rete avviata da questa applicazione.
   - **Personalizzato**: attività specifica da definire nella finestra di creazione della regola.
   - **<Modello>**: nome del modello che include l'insieme di regole solitamente applicate all'attività di rete dell'applicazione. Questo tipo di attività viene visualizzato nell'elenco se Kaspersky Anti-Virus include un modello appropriato per l'applicazione che ha avviato l'attività di rete. In tal caso, non sarà necessario personalizzare l'attività da consentire o bloccare. Utilizzando il modello verrà creato automaticamente un insieme di regole per l'applicazione.
3. Selezionare l'azione necessaria, ovvero **Permetti** o **Blocca**.

È importante ricordare che la regola creata verrà utilizzata solo quando tutti i parametri della connessione corrispondono. Non verrà invece applicata a una connessione stabilita, ad esempio, da una porta locale diversa.

Se non si desidera ricevere notifiche da Anti-Hacker quando le applicazioni tentano di stabilire connessioni di rete, utilizzare il collegamento **Disattiva modalità Training**. Successivamente, Anti-Hacker passerà in modalità **Protezione minima**, che consente tutte le connessioni di rete ad eccezione di quelle esplicitamente bloccate dalle regole.

RILEVAMENTO DELL'ATTIVITÀ DI RETE DI UN FILE ESEGUIBILE MODIFICATO

Se Anti-Hacker rileva un'attività di rete prodotta dal file eseguibile modificato di un programma avviato dall'utente, viene visualizzata una notifica speciale. Un file viene considerato modificato se è stato aggiornato o infettato da un programma dannoso.

La notifica contiene le informazioni seguenti:

- *Informazioni sul programma che ha avviato attività di rete* – nome e ID del processo, oltre al produttore del programma e numero di versione.
- *Azione* – serie di operazioni che il componente Kaspersky Anti-Virus deve eseguire per l'attività di rete rilevata.

Viene offerta di selezionare una delle azioni seguenti all'oggetto:

- **Permetti** – le informazioni sul file eseguibile modificato verranno aggiornate nell'ambito della regola esistente per l'applicazione. Inoltre, la sua attività di rete verrà consentita automaticamente.
- **Nega –** l'attività di rete verrà negata una volta.

RILEVAMENTO DI UNA NUOVA RETE

Ogni volta che il computer si connette a una nuova area, ad esempio una rete, viene visualizzata una notifica speciale.

La parte superiore della notifica contiene una breve descrizione della rete, che specifica l'indirizzo IP e la maschera di sottorete.

Nella parte inferiore della finestra viene richiesto di assegnare uno stato all'area e l'attività di rete viene consentita in base a tale stato:

- **Internet in Modalità Mascheramento (Blocca accesso esterno al computer)**. Questa funzione consente solo l'attività di rete avviata dall'utente o da un'applicazione consentita, cosicché il computer risulta invisibile per l'ambiente circostante. Questa modalità non pregiudica le prestazioni del computer su Internet.
- **Internet (Blocca condivisione file e stampante)**. Una rete ad alto rischio in cui il computer è esposto a qualsiasi tipo di minaccia. Si consiglia di selezionare questo stato per le reti non protette da applicazioni anti-virus, firewall, filtri e così via. Quando si seleziona tale stato, il programma garantisce la protezione massima per l'area in questione.
- **Rete locale (Consente l'accesso a file e stampanti)**. Questo stato è consigliabile per le aree con un fattore di rischio medio, ad esempio le reti LAN aziendali.
- **Rete attendibile (Consente qualsiasi attività di rete)**. Si consiglia di applicare questo stato alle aree che si ritiene siano assolutamente sicure e in cui il computer non è soggetto ad attacchi e tentativi di accesso ai dati.

Si sconsiglia l'uso della modalità Mascheramento se il computer viene utilizzato come server (ad esempio come server di posta o HTTP). Altrimenti i computer che si connettono al server non lo potranno visualizzare all'interno della rete.

RILEVAMENTO DI UN ATTACCO DI PHISHING

Ogni volta che Kaspersky Anti-Virus rileva un attacco di phishing, viene visualizzata una notifica speciale.

La notifica contiene le informazioni seguenti:

- Il nome della minaccia (*attacco di phishing*) come collegamento alla Virus Encyclopedia di Kaspersky Lab con una panoramica dettagliata della minaccia.
- Phishing dell'indirizzo del sito Web.
- Risposte possibili:
  - **Consenti**: il download del sito di phishing continua.
  - **Blocca**: il download del sito di phishing viene bloccato.

Per applicare l'azione selezionata a tutti gli oggetti con lo stesso stato rilevato nella sessione corrente del componente o dell'attività di protezione, selezionare la casella ☑ **Applica a tutti**. La sessione corrente corrisponde all'intervallo di tempo dall'avvio del componente fino alla sua disabilitazione o al suo riavvio o all'intervallo di tempo dall'inizio di una scansione anti-virus fino al suo completamento.

RILEVAMENTO DI UN TENTATIVO DI COMPOSIZIONE AUTOMATICA

Quando Anti-Spy rileva un certo numero di tentativi di composizione, viene visualizzata una notifica speciale con le informazioni seguenti:

- Il nome della minaccia così come è elencata nella Virus Encyclopedia di Kaspersky Lab. Il nome della minaccia viene specificato come collegamento al sito www.viruslist.com, in cui è possibile trovare informazioni dettagliate sul tipo di minaccia rilevata.
- Il nome completo del file del processo che ha avviato il tentativo di composizione e il relativo percorso.
- Informazioni sul numero di telefono chiamato dal dialer.
- Risposte possibili:
  - **Permetti**: viene consentita la composizione del numero specificato e la creazione della connessione di rete;
  - **Blocca**: la composizione del numero specificato viene bloccata;
  - **Aggiungi a numeri attendibili**: il numero viene aggiunto all'elenco di numeri attendibili. Questa opzione può essere utilizzata se la chiamata al numero specificato è stata autorizzata per evitare che l'applicazione generi falsi positivi ripetuti durante la composizione del numero.

RILEVAMENTO DI UN CERTIFICATO NON VALIDO

Il controllo di protezione per la connessione mediante il protocollo SSL viene eseguito utilizzando il certificato installato. Se viene rilevato un certificato non valido quando si tenta di stabilire la connessione al server, ad esempio se il certificato viene sostituito da un intruso, viene visualizzata una notifica.

La notifica conterrà informazioni sulle possibili cause dell'errore e identificherà l'indirizzo e la porta remoti. Verrà richiesto di decidere se continuare o meno la connessione con un certificato non valido:

- **Accetta certificato**: la connessione al sito Web continua;
- **Nega certificato**: la connessione al sito Web viene interrotta;
- **Visualizza certificato**: vengono visualizzate informazioni sul certificato.

UTILIZZO DELL'APPLICAZIONE DALLA RIGA DI COMANDO

Kaspersky Anti-Virus può essere utilizzato anche dalla riga di comando.

Sintassi della riga di comando:

```
avp.com <comando> [opzioni]
```

È necessario accedere all'applicazione dalla riga di comando dalla cartella di installazione Kaspersky Anti-Virus o specificando il percorso completo di avp.com.

È possibile utilizzare i seguenti comandi come <comando>:

- **HELP –** per indicazioni sulla sintassi dei comandi e sull'elenco dei comandi.
- **SCAN –** per la ricerca di malware negli oggetti.
- **UPDATE –** per avviare l'aggiornamento dell'applicazione.
- **ROLLBACK –** esegue il rollback dell'ultimo aggiornamento di Kaspersky Anti-Virus (il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia dell'applicazione).
- **START –** per avviare un componente o un'attività.
- **STOP –** per interrompere un componente o un'attività (il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia di Kaspersky Anti-Virus).
- **STATUS –** per visualizzare lo stato del componente o dell'attività corrente.
- **STATISTICS –** per visualizzare le statistiche del componente o dell'attività corrente.
- **EXPORT –** per esportare le impostazioni di protezione dell'applicazione.
- **IMPORT –** per importare le impostazioni di protezione di un componente o un'attività (il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia di Kaspersky Anti-Virus).
- **ACTIVATE –** per attivare Kaspersky Anti-Virus via Internet utilizzando il codice di attivazione.
- **ADDKEY –** per attivare l'applicazione utilizzando un file di chiave (il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia dell'applicazione).
- **RESTORE –** per ripristinare un file dalla quarantena.
- **EXIT –** per chiudere l'applicazione (il comando può essere eseguito solo se viene immessa la password assegnata tramite l'interfaccia dell'applicazione).
- **TRACE –** per ottenere un file di traccia.

Ogni comando richiede un insieme specifico di parametri.

IN QUESTA SEZIONE

Visualizzazione della Guida 199

Scansione anti-virus 199

Aggiornamento dell'applicazione 201

Rollback dell'ultimo aggiornamento 202

Avvio/arresto di un componente di protezione o di un'attività 202

Statistiche sul funzionamento di un componente o di un'attività 204

Esportazione delle impostazioni di protezione 204

Importazione delle impostazioni di protezione 204

Attivazione dell'applicazione 205

Ripristino di un file dalla quarantena 205

Chiusura dell'applicazione 205

Come ottenere un file di chiave 206

Codici restituiti della riga di comando 206

VISUALIZZAZIONE DELLA GUIDA

Questo comando consente di visualizzare la sintassi della riga di comando dell'applicazione:

```
avp.com [ /? | HELP ]
```

Per visualizzare la Guida per la sintassi di un comando specifico, è possibile utilizzare uno dei comandi seguenti:

```
avp.com <comando> /?
avp.com HELP <comando>
```

SCANSIONE ANTI-VIRUS

L'avvio della scansione anti-virus di una determinata area e l'elaborazione degli oggetti dannosi dalla riga di comando generalmente presenta la sintassi seguente:

```
avp.com SCAN [<oggetto esaminato>] [<azione>] [<tipi file>] [<esclusioni>]
[<impostazioni rapporti>] [<impostazioni avanzate>]
```

> Per esaminare gli oggetti, è inoltre possibile utilizzare le attività create nell'applicazione avviando quella richiesta dalla riga di comando. L'attività viene eseguita con le impostazioni specificate nell'interfaccia di Kaspersky Anti-Virus.

Descrizione delle impostazioni:

<oggetto esaminato>: questo parametro fornisce l'elenco di oggetti che verranno esaminati per rilevare eventuale codice dannoso. Può includere diversi valori dell'elenco fornito separati da spazi:

- **<file>** – elenco di percorsi dei file e/o delle cartelle da esaminare. È possibile indicare un percorso assoluto o relativo. Gli elementi dell'elenco devono essere separati da uno spazio. Commenti:
  - se il nome dell'oggetto contiene uno spazio, deve essere incluso tra virgolette;
  - se viene fatto riferimento a una cartella specifica, verranno esaminati tutti i file in essa contenuti.
- **/ALL** – scansione completa del computer.
- **/MEMORY** – oggetti della RAM.
- **/STARTUP** – oggetti di avvio.
- **/MAIL** – database di posta elettronica.
- **/REMDRIVES** – tutte le unità rimovibili.
- **/FIXDRIVES** – tutte le unità locali.
- **/NETDRIVES** – tutte le unità di rete.
- **/QUARANTINE** – oggetti in quarantena.
- **/@:<filelist.lst>** – percorso del file contenente un elenco di oggetti e cataloghi da esaminare. Il file deve essere in formato testo e ogni oggetto della scansione deve essere elencato in una riga separata. È possibile indicare un percorso assoluto o relativo. Il percorso deve essere inserito tra virgolette anche se contiene spazi.

<azione>: questo parametro determina le azioni che verranno eseguite sugli oggetti dannosi rilevati durante la scansione. Se non è definito, l'azione predefinita è quella con il valore **/i2**. Sono possibili i valori seguenti:

- **/i0** – nessuna azione sull'oggetto; solo registrazione delle informazioni nel rapporto.
- **/i1** – gli oggetti infetti vengono elaborati e, se la disinfezione è impossibile, vengono ignorati.
- **/i2** – gli oggetti infetti vengono elaborati e, se la disinfezione non riesce, vengono eliminati. Non vengono eliminati gli oggetti infetti appartenenti a oggetti compositi. Vengono eliminati gli oggetti composti con intestazione eseguibile (archivi .sfx). Per impostazione predefinita.
- **/i3** – gli oggetti infetti vengono elaborati e, se la disinfezione non riesce, vengono eliminati. Vengono eliminati tutti gli oggetti composti se non è possibile eliminare le parti infette.
- **/i4** – gli oggetti infetti vengono eliminati. Vengono eliminati tutti gli oggetti composti se non è possibile eliminare le parti infette.
- **/i8 –** viene richiesto l'intervento dell'utente se viene rilevato un oggetto infetto.
- **/i9** – viene richiesto l'intervento dell'utente al termine della scansione.

<tipi file>: questo parametro definisce i tipi di file che saranno sottoposti alla scansione anti-virus. Per impostazione predefinita, questo parametro non è specificato e sono sottoposti a scansione solo i file infetti in base al contenuto. Sono possibili i valori seguenti:

- **/fe** – vengono esaminati solo i file infetti in base all'estensione.
- **/fi** – vengono esaminati solo i file infetti in base al contenuto.
- **/fa** – vengono esaminati tutti i file.

<esclusioni>: questo parametro definisce gli oggetti esclusi dalla scansione. Può includere diversi valori dell'elenco fornito separati da spazi.

- **/e:a** – non vengono esaminati gli archivi.
- **/e:b** – non vengono esaminati i database di posta elettronica.
- **/e:m** – non vengono esaminati i messaggi di posta con testo semplice.
- **/e:<maschera>** – non vengono esaminati gli oggetti corrispondenti alla maschera.
- **/e:<secondi>** – vengono ignorati gli oggetti la cui scansione richiede un intervallo di tempo superiore a quello specificato nel parametro **<secondi>**.

<impostazioni rapporti>: questo parametro determina il formato del rapporto sui risultati della scansione. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.

- **/R:<file_rapporto>** – in questo file vengono registrati solo gli eventi importanti.
- **/RA:<file_rapporto>** – in questo file vengono registrati tutti gli eventi.

<impostazioni avanzate> – impostazioni che definiscono l'utilizzo delle tecnologie di scansione anti-virus e del file di configurazione delle impostazioni:

- **/iChecker=<abilitato|disabilitato>** – viene abilitato/disabilitato l'utilizzo della tecnologia iChecker.
- **/iSwift=<abilitato|disabilitato>** – viene abilitato/disabilitato l'utilizzo della tecnologia /iSwift.
- **/C:<nome_file_configurazione>** – definisce il percorso del file di configurazione che contiene le impostazioni di scansione dell'applicazione. È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono utilizzati i valori impostati nell'interfaccia dell'applicazione.

Esempi:

- *Avviare una scansione di memoria, oggetti di avvio, database di posta elettronica, directory Documenti e Programmi e file test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\Documenti"
"C:\Programmi" "C:\Downloads\test.exe"
```

- *Scansione degli oggetti elencati nel file object2scan.txt mediante il file di configurazione scan_setting.txt per l'operazione. Utilizzo del file di configurazione scan_setting.txt. Al termine della scansione, creare un rapporto per registrare tutti gli eventi:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

File di configurazione di esempio:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

AGGIORNAMENTO DELL'APPLICAZIONE

La sintassi per l'aggiornamento dei moduli e dei database di Kaspersky Anti-Virus dalla riga di comando è la seguente:

```
avp.com UPDATE [<sorgente_aggiornamento>] [/APP=<abilitato|disabilitato>]
[<impostazioni_rapporti>] [<impostazioni_avanzate>]
```

Descrizione delle impostazioni:

<sorgente_aggiornamento> – server HTTP o FTP o cartella di rete per il download degli aggiornamenti. Se non viene selezionato un percorso, la sorgente degli aggiornamenti sarà quella delle impostazioni di aggiornamento dell'applicazione.

/APP=<abilitato|disabilitato> – abilita / disabilita l'aggiornamento dei moduli dell'applicazione.

<impostazioni rapporti>: questo parametro determina il formato del rapporto sui risultati della scansione. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi. Sono possibili i valori seguenti:

- **/R:<file_rapporto>** – in questo file vengono registrati solo gli eventi importanti.
- **/RA:<file_rapporto>** – in questo file vengono registrati tutti gli eventi.

<impostazioni avanzate> – impostazioni che definiscono l'utilizzo delle tecnologie di scansione anti-virus.

/C:<nome_file_configurazione> – definisce il percorso del file di configurazione che contiene le impostazioni di scansione dell'applicazione. È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono utilizzati i valori impostati nell'interfaccia dell'applicazione.

Esempi:

aggiornamento dei database dell'applicazione e registrazione di tutti gli eventi in un rapporto:

```
avp.com UPDATE /RA:avbases_upd.txt
```

Aggiornamento dei moduli di Kaspersky Anti-Virus mediante i parametri del file di configurazione updateapp.ini:

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

ROLLBACK DELL'ULTIMO AGGIORNAMENTO

Sintassi del comando:

```
avp.com ROLLBACK </password=<password>> [<impostazioni_rapporto>]
```

Descrizione delle impostazioni:

</password=<password>> – password assegnata mediante l'interfaccia dell'applicazione. Il comando ROLLBACK non verrà eseguito senza l'immissione di una password.

<impostazioni rapporti> – questo parametro determina il formato del rapporto sui risultati della scansione. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.

- **/R:<file_rapporto>** – in questo file vengono registrati solo gli eventi importanti.
- **/RA:<file_rapporto>** – in questo file vengono registrati tutti gli eventi. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.

Esempio:

```
avp.com ROLLBACK/password=123/RA:rollback.txt
```

AVVIO/ARRESTO DI UN COMPONENTE DI PROTEZIONE O DI UN'ATTIVITÀ

Sintassi del comando START:

```
avp.com START <profilo|nome_attività> [<impostazioni_rapporto>]
```

Sintassi del comando STOP:

```
avp.com STOP <profilo|nome_attività> </password=<password>>
```

Descrizione delle impostazioni:

</password=<password>> – password assegnata mediante l'interfaccia dell'applicazione. Il comando STOP non verrà eseguito senza l'immissione di una password.

<impostazioni rapporti> – questo parametro determina il formato del rapporto sui risultati della scansione. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi. Sono possibili i valori seguenti:

- **/R:<file_rapporto>** – in questo file vengono registrati solo gli eventi importanti.
- **/RA:<file_rapporto>** – in questo file vengono registrati tutti gli eventi. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, sullo schermo vengono visualizzati i risultati della scansione e tutti gli eventi.

L'impostazione **<profilo|nome_attività>** può contenere uno dei valori seguenti:

- **Protection (RTP)** – tutti i computer di protezione;
- **Anti-Hacker (AH)** – Anti-Hacker;
- **fw** - Firewall;
- **ids** - istema rilevamento intrusioni;
- **Anti-Spam (AS)** – Anti-Spam;
- **Anti-Spy (ASPY)** – Anti-Spy;
- **AdBlocker** - Anti-Banner;
- **antidial** - Anti-Dialer;
- **Behavior_Blocking2** – Difesa Proattiva;
- **pdm2** - isi Attività Applicazione;
- **regguard2** - Controllo del Registro;
- **File_Monitoring (FM)** – Anti-Virus File;
- **Web_Monitoring** – Anti-Virus Web;
- **Mail_Monitoring (EM)** – Anti-Virus Posta;
- **Lock_Control (LC)** – controllo accesso;
- **Device_Locker** – controllo dispositivo;
- **Scan_My_Computer** – attività di scansione completa del computer;
- **Scan_Objects** – scansione di oggetti;
- **Scan_Quarantine** – scansione della quarantena;
- **Scan_Startup (STARTUP)** – scansione degli oggetti di avvio;
- **Updater** – attività di aggiornamento;

- **Rollback** – attività di rollback degli aggiornamenti.

I componenti e le attività avviati dalla riga di comando vengono eseguiti con le impostazioni modificate nell'interfaccia dell'applicazione.

Esempi:

Per abilitare Anti-Virus File, digitare quanto segue nel prompt dei comandi:

```
avp.com START FM
```

Per arrestare l'attività di scansione dal prompt dei comandi, immettere:

```
avp.com STOP SCAN_MY_COMPUTER /password=<password>
```

STATISTICHE SUL FUNZIONAMENTO DI UN COMPONENTE O DI UN'ATTIVITÀ

Sintassi del comando STATUS:

```
avp.com STATUS <profilo|nome_attività>
```

Sintassi del comando STATISTICS:

```
avp.com STATISTICS <profilo|nome_attività>
```

Descrizione delle impostazioni:

L'impostazione **<profilo|nome_attività>** può contenere uno dei valori specificati nei comandi START / STOP (vedere a pag. 202).

ESPORTAZIONE DELLE IMPOSTAZIONI DI PROTEZIONE

Sintassi del comando:

```
avp.com EXPORT <profilo|nome_attività> <nome_file>
```

Descrizione delle impostazioni:

L'impostazione **<profilo|nome_attività>** può contenere uno dei valori specificati nei comandi START / STOP (vedere a pag. 202).

<nome_file> – percorso nel quale verranno esportate le impostazioni dell'applicazione. È possibile specificare un percorso assoluto o relativo.

Esempio:

```
avp.com EXPORT RTP RTP_settings.dat - formato binario
avp.com EXPORT FM FM_settings.txt – formato testo
```

IMPORTAZIONE DELLE IMPOSTAZIONI DI PROTEZIONE

Sintassi del comando:

```
avp.com IMPORT <nome_file> </password=<password_utente>>
```

Descrizione delle impostazioni:

<nome_file> – percorso nel quale verranno importate le impostazioni dell'applicazione. È possibile specificare un percorso assoluto o relativo.

</password=<password_utente>> – password assegnata mediante l'interfaccia dell'applicazione.

Esempio:

```
avp.com IMPORT settings.dat
```

ATTIVAZIONE DELL'APPLICAZIONE

Kaspersky Anti-Virus può essere attivato in due modi:

- tramite Internet utilizzando un codice di attivazione (comando ACTIVATE)
- utilizzando un file di chiave della licenza (comando ADDKEY).

Sintassi del comando:

```
avp.com ACTIVATE <codice_attivazione> </password=<password>>
avp.com ADDKEY <nome_file> </password=<password>>
```

Descrizione delle impostazioni:

<codice_attivazione> – il codice di attivazione: xxxxx-xxxxx-xxxxx-xxxxx.

<nome_file> – file di chiave dell'applicazione con estensione .key: xxxxxxxx.key.

</password=<password>> – password assegnata mediante l'interfaccia dell'applicazione.

Esempio:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key </password=<password>>
```

RIPRISTINO DI UN FILE DALLA QUARANTENA

Sintassi del comando:

```
avp.com RESTORE [/REPLACE] <nome_file>
```

Descrizione delle impostazioni:

/REPLACE – sostituzione di un file esistente.

<nome_file> – nome del file da ripristinare.

Esempio:

```
avp.com REPLACE C:\eicar.com
```

CHIUSURA DELL'APPLICAZIONE

Sintassi del comando:

```
avp.com EXIT </password=<password>>
```

Descrizione delle impostazioni:

</password=<password>> – password assegnata mediante l'interfaccia dell'applicazione. Il comando non verrà eseguito senza l'immissione di una password.

COME OTTENERE UN FILE DI CHIAVE

Se si verificano problemi con Kaspersky Anti-Virus, potrebbe essere necessario creare un file di traccia. I file di traccia sono utili per individuare il problema con maggiore precisione e vengono molto utilizzati dagli esperti dell'Assistenza tecnica.

Sintassi del comando:

```
avp.com TRACE [file] [on|off] [<livello_traccia>]
```

Descrizione delle impostazioni:

[abilitato|disabilitato] – abilita / disabilita la creazione del file di traccia.

[file] – copia la traccia in un file.

<livello_traccia> – questo valore può essere un numero intero compreso tra 100 (livello minimo, solo messaggi critici) e 600 (livello massimo, tutti i messaggi).

Se si contatta il servizio di assistenza tecnica, occorre specificare il livello di traccia necessario. Se non viene specificato alcun livello, si consiglia di impostare il valore su 500.

Esempi:

➡ *Per disabilitare la creazione del file di traccia:*

```
avp.com TRACE file off
```

➡ *Creare un file di traccia con un livello di 500:*

```
avp.com TRACE file on 500
```

CODICI RESTITUITI DELLA RIGA DI COMANDO

I codici generali possono essere restituiti da qualsiasi comando dalla riga di comando. I codici restituiti comprendono i codici generali nonché quelli relativi a un tipo specifico di attività.

Codici restituiti generali:

- 0 – operazione completata con successo;
- 1 – valore non valido per l'impostazione;
- 2 – errore sconosciuto;
- 3 – errore di completamento dell'attività;
- 4 – attività annullata.

Codici restituiti dall'attività di scansione anti-virus:

- 101 – tutti gli oggetti pericolosi sono stati elaborati;
- 102 – rilevamento di oggetti pericolosi.

MODIFICA, RIPARAZIONE E RIMOZIONE DELL'APPLICAZIONE

L'applicazione può essere disinstallata nei modi seguenti:

- tramite l'installazione guidata dell'applicazione (vedere la sezione "Modifica, riparazione e rimozione dell'applicazione tramite l'installazione guidata" a pagina 207);
- dalla riga di comando (vedere la sezione "Rimozione dell'applicazione dalla riga di comando" a pagina 209);
- tramite Kaspersky Administration Kit (vedere la Guida di distribuzione di Kaspersky Administration Kit);
- tramite i criteri di gruppo di dominio di Microsoft Windows Server 2000/2003 (vedere la sezione "Disinstallazione dell'applicazione" a pagina 26).

IN QUESTA SEZIONE

Modifica, riparazione e rimozione dell'applicazione tramite l'installazione guidata 207

Rimozione dell'applicazione dalla riga di comando 209

MODIFICA, RIPARAZIONE E RIMOZIONE DELL'APPLICAZIONE TRAMITE L'INSTALLAZIONE GUIDATA

In caso di errori di funzionamento dovuti a una configurazione errata o alla corruzione dei file può rendersi necessario riparare l'applicazione.

La modifica dei componenti dell'applicazione consente di installare componenti di Kaspersky Anti-Virus assenti o di eliminare quelli indesiderati o non necessari.

➡ *Per riparare o modificare i componenti assenti di Kaspersky Anti-Virus o disinstallare l'applicazione, eseguire le operazioni seguenti:*

1. Inserire il CD di installazione nell'unità CD/DVD-ROM (se utilizzato per installarel'applicazione. Se Kaspersky Anti-Virus è stato installato da una fonte diversa (cartella ad accesso pubblico, cartella nel disco fisso, ecc.), verificare che il pacchetto di installazione dell'applicazione si trovi nello stesso percorso e di potervi accedere.
2. Selezionare **Start** → **Tutti i programmi** → **Kaspersky Anti-Virus 6.0 per Windows Workstations MP4** → **Modifica, ripara** o **rimuovi**.

Si aprirà l'installazione guidata del programma. Di seguito vengono illustrate in modo dettagliato le procedure per la riparazione, la modifica o la rimozione dell'applicazione.

PASSAGGIO 1. FINESTRA INIZIALE DELL'INSTALLAZIONE

Dopo aver eseguito tutti i passaggi sopra descritti, necessari per riparare o modificare l'applicazione, si apre la finestra iniziale di installazione di Kaspersky Anti-Virus. Fare clic sul pulsante **Avanti** per continuare.

PASSAGGIO 2. SELEZIONE DI UN'OPERAZIONE

In questa fase viene chiesto di selezionare l'operazione che si desidera eseguire sull'applicazione. È possibile modificare i componenti dell'applicazione, riparare quelli già installati, rimuoverne alcuni o l'intera applicazione. Per eseguire l'operazione desiderata, fare clic sul pulsante corrispondente. Il programma di installazione si comporterà diversamente in base all'operazione selezionata.

La modifica dell'applicazione è analoga all'installazione personalizzata, in cui è possibile specificare quali componenti si desidera installare e quali eliminare.

La riparazione dell'applicazione dipende dai componenti installati. Saranno riparati i file di tutti i componenti installati e per ciascuno di essi sarà impostato il livello di protezione **Consigliato**.

Quando si rimuove l'applicazione è possibile selezionare quali dati creati e usati dall'applicazione si desidera salvare nel computer. Per eliminare tutti i dati di Kaspersky Anti-Virus, selezionare l'opzione **Disinstallazione completa**. Per salvare i dati, selezionare l'opzione **Salva oggetti applicazione** e specificare quali oggetti non devono essere eliminati:

- *Informazioni sull'attivazione* – file chiave necessario per il funzionamento dell'applicazione.

Database dell'applicazione – serie completa delle firme di programmi pericolosi, virus e altre minacce correnti alla data dell'ultimo aggiornamento.

- *Database di Anti-Spam* – database utilizzato per individuare la posta indesiderata. Questo database contiene informazioni dettagliate su quali messaggi costituiscono spam e quali no.
- *Backup oggetti* – copie di backup di oggetti eliminati o disinfettati. Si consiglia di salvare questi oggetti per poterli eventualmente ripristinare in un secondo momento.
- *Oggetti in quarantena* – oggetti potenzialmente infetti da virus o varianti di essi. Questi oggetti contengono codici simili a quelli di virus noti ma è difficile stabilire se siano dannosi. Si consiglia di salvare questi oggetti poiché potrebbero rivelarsi innocui oppure essere disinfettati dopo l'aggiornamento delle firme delle minacce.
- *Impostazioni dell'applicazione* – impostazioni per tutti i componenti dell'applicazione.
- *Dati iSwift* – database contenente informazioni sugli oggetti esaminati nei file system NTFS. Questi dati possono aumentare la velocità di scansione. Usando questo database, Kaspersky Anti-Virus esamina solo i file che hanno subito delle modifiche dopo l'ultima scansione.

Se trascorre molto tempo tra la disinstallazione di una versione di Kaspersky Anti-Virus e l'installazione di un'altra, si sconsiglia di utilizzare il database iSwift creato da un'installazione precedente dell'applicazione. Un programma dannoso potrebbe infatti essere penetrato nel computer nel frattempo e i suoi effetti non sarebbero rilevati dal database, con conseguente rischio di infezione.

Per avviare l'operazione selezionata, fare clic sul pulsante **Avanti**. L'applicazione inizierà a copiare i file necessari nel computer o a eliminare i componenti e i dati selezionati.

PASSAGGIO 3. COMPLETAMENTO DELLA MODIFICA, RIPARAZIONE O RIMOZIONE DELL'APPLICAZIONE

L'avanzamento del processo di modifica, riparazione o rimozione dell'applicazione viene visualizzato sullo schermo. Al termine, l'utente viene informato del completamento dell'operazione.

La rimozione del programma richiede solitamente il riavvio del computer, necessario per applicare le modifiche al sistema. L'applicazione chiederà quindi se si desidera riavviare il computer. Fare clic sul pulsante **Sì** per riavviarlo subito. Per riavviarlo in un secondo momento, fare clic sul pulsante **No**.

RIMOZIONE DELL'APPLICAZIONE DALLA RIGA DI COMANDO

- *Per disinstallare Kaspersky Anti-Virus 6.0 for for Windows Workstations MP4 dalla riga di comando, eseguire quanto indicato di seguito:*

  ```
  msiexec /x <package_name>
  ```

  Si aprirà l'installazione guidata. che consente di disinstallare l'applicazione.

- *Per disinstallare l'applicazione in modalità non interattiva senza riavviare il computer (il computer dovrà essere riavviato manualmente dopo la disinstallazione), digitare:*

  ```
  msiexec /x <package_name> /qn
  ```

- *Per disinstallare l'applicazione in modalità non interattiva e riavviare il computer al termine dell'operazione, digitare:*

  ```
  msiexec /x <package_name> ALLOWREBOOT=1 /qn
  ```

Se durante l'installazione dell'applicazione si è scelto di proteggerla dalla disinstallazione tramite una password, è necessario confermare tale password quando la si disinstalla. In caso contrario, sarà impossibile disinstallare l'applicazione.

- *Per rimuovere l'applicazione quando è protetta da una password, digitare:*

  `msiexec /x <package_name> KLUNINSTPASSWD=******` – per rimuovere l'applicazione in modalità interattiva;

  `msiexec /x <package_name> KLUNINSTPASSWD=****** /qn` – per rimuovere l'applicazione in modalità non interattiva.

GESTIONE DELL'APPLICAZIONE TRAMITE KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit è un sistema che consente di centralizzare la gestione delle principali attività amministrative utilizzate in un sistema di protezione per una rete aziendale, basato sulle applicazioni incluse in Kaspersky Anti-Virus Open Space Security. Kaspersky Administration Kit supporta tutte le configurazioni di rete basate sul protocollo TCP.

L'applicazione è destinata agli amministratori di reti aziendali e ai dipendenti responsabili della protezione anti-virus nelle rispettive aziende.

Kaspersky Anti-Virus 6.0 per Windows Workstations MP4 è uno dei prodotti Kaspersky Lab che può essere gestito tramite l'interfaccia dell'applicazione, il prompt dei comandi (questi metodi sono descritti nella presente documentazione) o utilizzando il programma Kaspersky Administration Kit (se il computer è incluso in un sistema di amministrazione remota centralizzato).

Per gestire Kaspersky Anti-Virus tramite Kaspersky Administration Kit, eseguire le seguenti operazioni:

- distribuire il *Administration Server* nella rete;
- installare Administration Console nella workstation dell'amministratore (per ulteriori informazioni consultare il manuale di distribuzione di Kaspersky Administration Kit);
- installare Kaspersky Anti-Virus e *Network Agent* (fornito con Kaspersky Administration Kit) nei computer della rete. Per ulteriori informazioni sull'installazione remota del pacchetto di installazione di Kaspersky Anti-Virus nei computer in rete, consultare il manuale per la distribuzione di Kaspersky Administration Kit.

Se nei computer della rete è già installata la versione precedente di Kaspersky Anti-Virus, è necessario eseguire la procedura seguente prima di eseguire l'aggiornamento alla nuova versione tramite Kaspersky Administration Kit:

- Sospendere la versione precedente dell'applicazione (è possibile eseguire questa operazione in remoto tramite Kaspersky Administration Kit);
- Chiudere tutte le applicazioni in esecuzione prima di iniziare l'installazione;
- Dopo aver completato l'installazione, riavviare il sistema operativo nel computer remoto.

Prima di aggiornare il plug-in di amministrazione di Kaspersky Lab tramite Kaspersky Administration Kit, chiudere Administration Console.

La console di amministrazione (vedere la figura seguente) consente di gestire l'applicazione tramite Kaspersky Administration Kit. Costituisce un'interfaccia standard integrata in MMC e consente all'amministratore di eseguire le funzioni seguenti:

- Installazione e disinstallazione remota di Kaspersky Anti-Virus e di *Network Agent* nei computer della rete;
- Configurazione remota di Kaspersky Anti-Virus nei computer della rete;
- Aggiornamento dei database e moduli di Kaspersky Anti-Virus;
- Gestione delle licenze per Kaspersky Anti-Virus nei computer della rete;
- Visualizzazione di informazioni sul funzionamento dell'applicazione nei computer client.

Fig. 12. La console di amministrazione di Kaspersky Administration Kit.

L'aspetto della finestra principale del Kaspersky Administration Kit varia in relazione al sistema operativo del computer in uso.

Quando si utilizza Kaspersky Administration Kit, l'applicazione viene gestita tramite le impostazioni delle regole, delle attività e dell'applicazione definite dall'amministratore.

Le azioni eseguite dell'applicazione vengono definite *attività*. In base alle funzioni che eseguono, le attività si suddividono in *tipi*: attività di scansione anti-virus, attività di aggiornamento dell'applicazione, rollback degli aggiornamenti e attività di installazione del file di chiave.

Ogni attività prevede una serie di impostazioni per l'applicazione che vengono utilizzate quando viene eseguita. Le impostazioni dell'attività per l'applicazione che sono comuni a tutti i tipi di attività sono definiti *impostazioni dell'applicazione*. Le impostazioni dell'applicazione che sono specifiche per un tipo di attività costituiscono le *impostazioni dell'attività*. Le impostazioni dell'applicazione e le impostazioni dell'attività non si sovrappongono.

La funzione chiave dell'amministrazione centralizzata consiste nel raggruppare computer remoti nella rete e gestirli creando e configurando criteri di gruppo.

Un criterio è una serie di impostazioni dell'applicazione per un gruppo, nonché una serie di restrizioni alla modifica di tali impostazioni durante la configurazione dell'applicazione o delle attività in un singolo computer client. Un criterio include impostazioni per la configurazione di tutte le funzioni, dell'applicazione ad eccezione delle impostazioni personalizzate per istanze specifiche di un'attività. ad esempio le impostazioni di pianificazione.

Di conseguenza, i criteri includono le seguenti impostazioni:

- Impostazioni comuni a tutte le attività (impostazioni dell'applicazione);

- Impostazioni comuni a tutte le istanze di un singolo tipo di attività (impostazioni principali di un'attività).

Di conseguenza, un criterio per Kaspersky Anti-Virus, le cui attività includono la protezione e la scansione anti-virus, include tutte le impostazioni necessarie per configurare l'applicazione quando si eseguono entrambi i tipi di attività, ma non include, ad esempio, una pianificazione per l'esecuzione di tali attività o le impostazioni che definiscono l'ambito della scansione.

IN QUESTA SEZIONE

Gestione dell'applicazione 212

Gestione delle attività 218

Gestione dei criteri 224

GESTIONE DELL'APPLICAZIONE

Kaspersky Administration Kit offre l'opportunità di avviare e terminare Kaspersky Anti-Virus in remoto su singoli computer client, nonché di modificare le impostazioni generali per l'applicazione, ad esempio abilitando/disabilitando la protezione del computer, modificando le impostazioni per il backup, la quarantena e la creazione di rapporti.

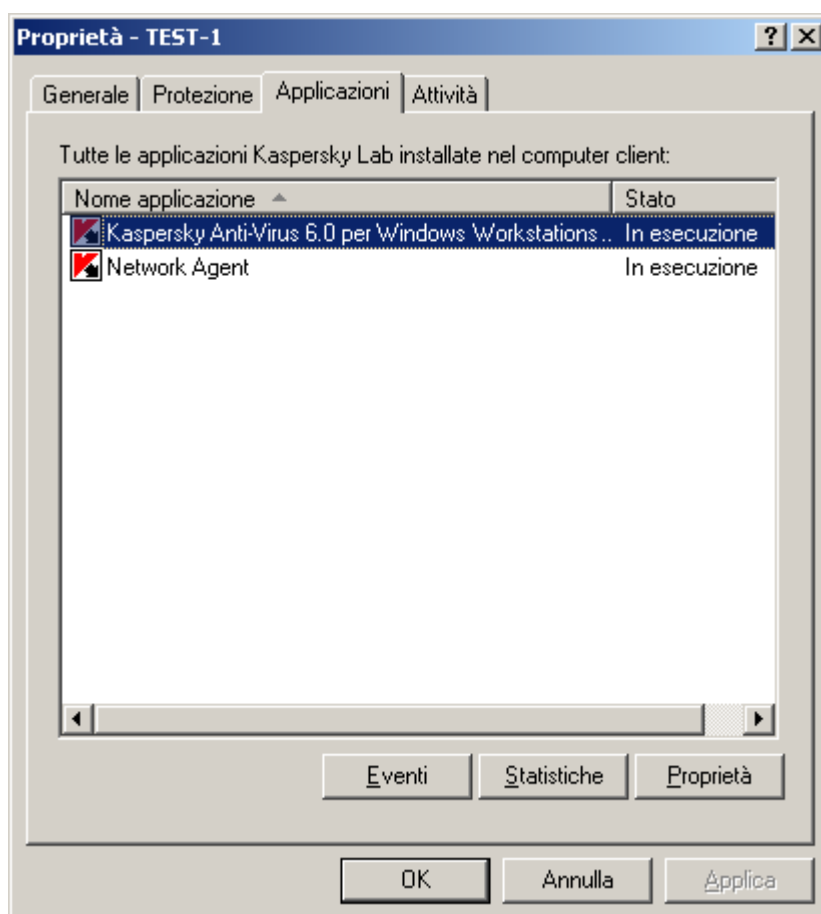



*Fig. 13. Finestra delle proprietà del computer client. Scheda **Applicazioni***

Per gestire le impostazioni dell'applicazione, eseguire le seguenti operazioni:

1. Aprire Administration Console di Kaspersky Administration Kit.

2. Selezionare la cartella **Computer gestiti** con il nome del gruppo che include il computer client.

3. Nel gruppo selezionato, aprire la cartella **Computer client** e selezionare il computer per cui modificare le impostazioni dell'applicazione.

4. Selezionare il comando **Proprietà** dal menu di scelta rapida o la voce corrispondente nel menu **Azione** per aprire la finestra delle proprietà del computer client.

5. Nella scheda **Applicazioni** nella finestra delle proprietà del computer client viene visualizzato l'elenco completo delle applicazioni Kaspersky Lab installate nel computer client. Selezionare **Kaspersky Anti-Virus 6.0 per Windows Workstations MP4** nell'elenco delle applicazioni.

   In questo elenco di applicazioni sono disponibili controlli che consentono di:

   - Visualizzare l'elenco di eventi verificatisi durante il funzionamento dell'applicazione nel computer client e registrati nel Administration Server;
   - Visualizzare le statistiche correnti sul funzionamento dell'applicazione;
   - Modificare le impostazioni dell'applicazione (vedere a pag. 215).

AVVIO E ARRESTO DELL'APPLICAZIONE

Kaspersky Anti-Virus 6.0 può essere installato e avviato nei computer clienti dalla finestra delle proprietà dell'applicazione (vedere la figura seguente).

Nella parte superiore della finestra è presente il nome dell'applicazione installata, le informazioni sulla versione, la data di installazione, lo stato (se l'applicazione è in esecuzione o è stata terminata nel computer locale) e informazioni sullo stato del database delle firme delle minacce.

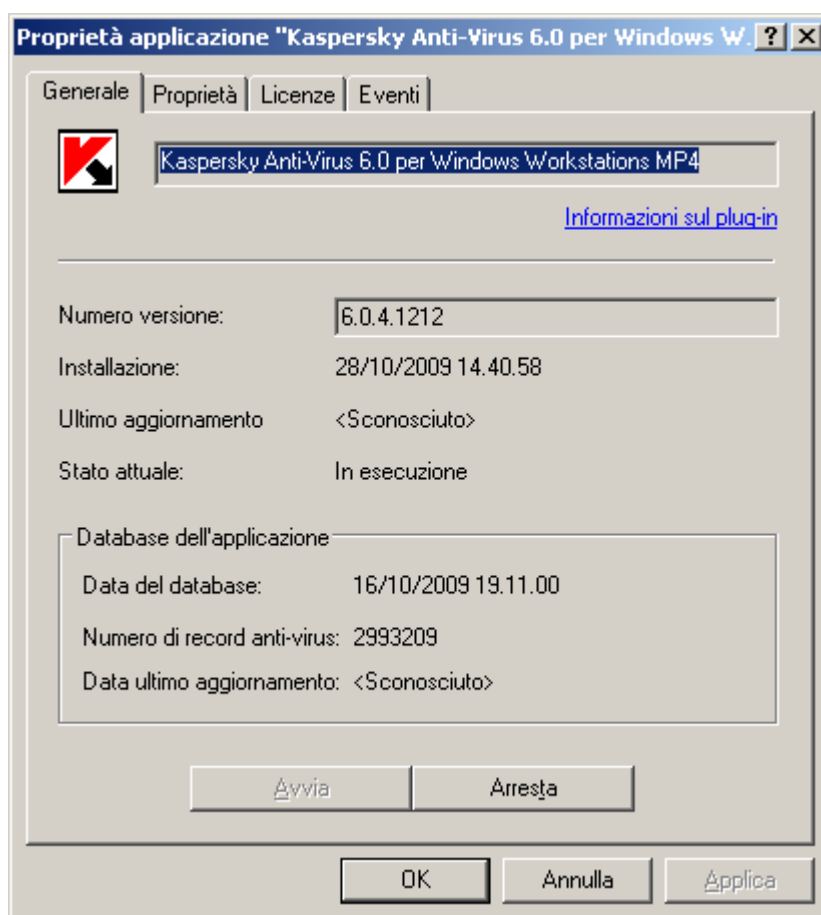



Fig. 14. Finestra delle proprietà dell'applicazione. Scheda ***Generale***

➧ *Per terminare o avviare l'applicazionein un computer remoto, eseguire le seguenti operazioni:*

1. Aprire la scheda **Applicazioni** nella finestra delle proprietà del computer client (vedere pagina 212).
2. Selezionare **Kaspersky Anti-Virus 6.0 per Windows Workstations MP4** nell'elenco delle applicazioni e cliccare sul pulsante **Proprietà**.
3. Nella finestra delle proprietà dell'applicazione che verrà visualizzata cliccare sul pulsante **Termina** nella scheda **Generale** per arrestare l'applicazione o il pulsante **Avvia** per avviarla.

CONFIGURAZIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE

È possibile visualizzare e modificare le impostazioni dell'applicazione nella scheda **Proprietà** della finestra delle proprietà dell'applicazione (vedere la figura seguente). Le altre schede sono standard per l'applicazione Kaspersky Administration Kit e sono descritte in maggiore dettaglio nel manuale di riferimento.

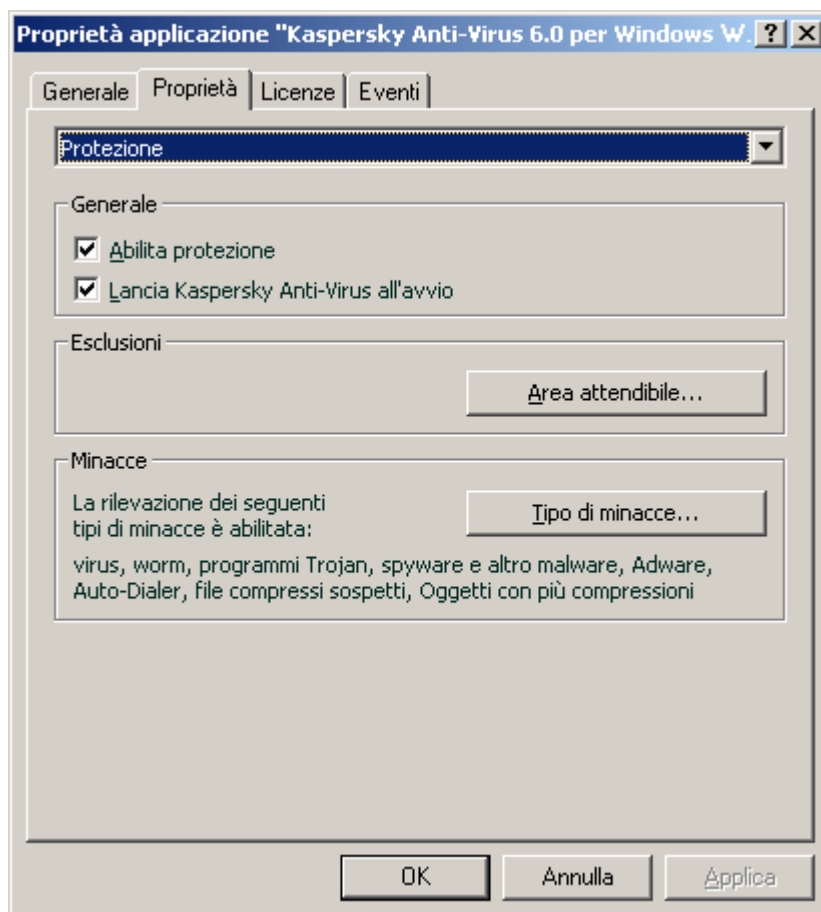



*Fig. 15. Finestra delle proprietà dell'applicazione. Scheda **Proprietà***

Se è stato creato un criterio per l'applicazione (vedere pagina 225) che impedisce di modificare alcune impostazioni, non sarà possibile modificarle durante la configurazione dell'applicazione.

Per visualizzare e modificare l'applicazione eseguire le seguenti operazioni:

1. Aprire la scheda **Applicazioni** nella finestra delle proprietà del computer client (vedere pagina 212).
2. Selezionare **Kaspersky Anti-Virus 6.0 per Windows Workstations MP4** nell'elenco delle applicazioni e cliccare sul pulsante **Proprietà**.
3. Nella finestra delle proprietà dell'applicazione visualizzata, all'interno della scheda **Proprietà**, è possibile modificare le impostazioni generali di Kaspersky Anti-Virus, le impostazioni di archiviazione e di creazione rapporti, nonché le impostazioni di rete. A tale scopo, selezionare il valore richiesto nel menu a discesa nella parte superiore della finestra e modificare le impostazioni.

CONFIGURAZIONE DI IMPOSTAZIONI SPECIFICHE

Quando si gestisce Kaspersky Anti-Virus tramite Kaspersky Administration Kit, è possibile abilitare/disabilitare l'interattività, configurare l'aspetto dell'applicazione e modificare le informazioni relative all'assistenza tecnica. Queste impostazioni possono essere modificate nella finestra delle proprietà dell'applicazione (vedere la figura seguente).

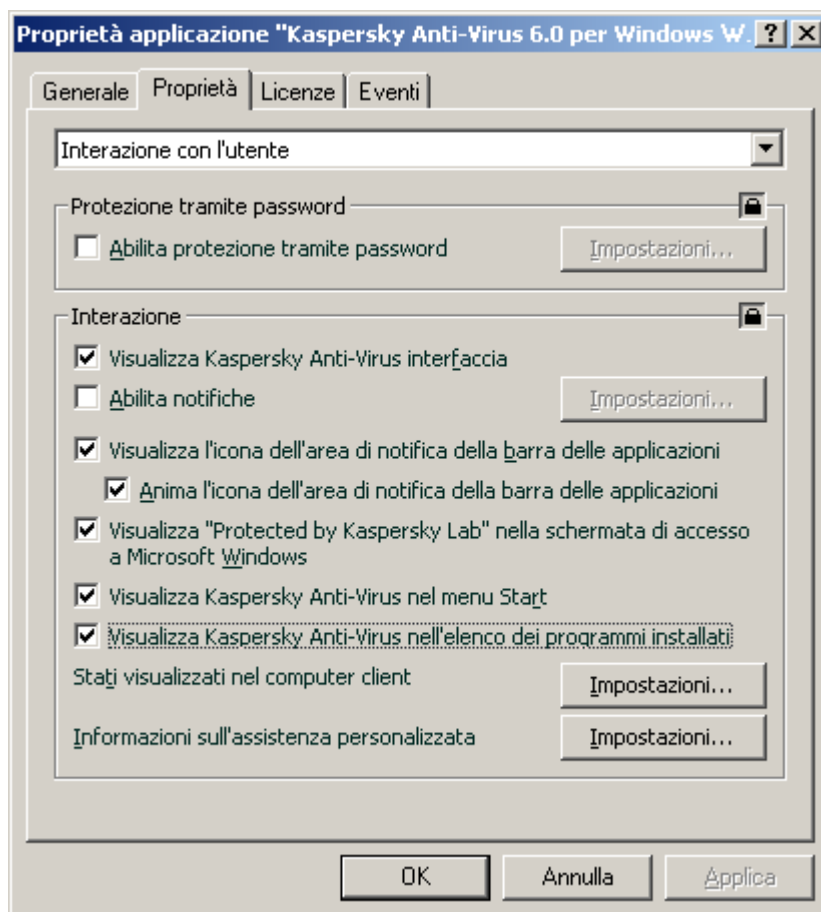



Fig. 16. Finestra delle proprietà dell'applicazione. Configurazione di impostazioni specifiche

Nella sezione **Interazione** è possibile specificare le impostazioni per l'interazione dell'utente con l'interfaccia di Kaspersky Anti-Virus:

- *Visualizzazione dell'interfaccia dell'applicazione in un computer remoto*. Se la casella ☑ **Visualizza interfaccia di Kaspersky Anti-Virus** è selezionata, gli utenti che lavorano su un computer remoto vedranno l'icona di Kaspersky Anti-Virus e i messaggi a comparsa. Avranno inoltre la possibilità di decidere le azioni ulteriori nella finestra di notifica in cui vengono segnalati gli eventi. Per disabilitare la modalità interattiva del funzionamento dell'applicazione, deselezionare la casella.

- *Notifiche degli eventi*. È inoltre possibile configurare i parametri delle notifiche relative agli eventi nel funzionamento dell'applicazione, ad esempio il rilevamento di oggetti pericolosi. A tal fine, selezionare la casella ☑ **Abilita notifiche** e cliccare sul pulsante **Impostazioni**.

- *Visualizzazione dell'icona dell'applicazione nell'area di notifica della barra delle applicazioni e della relativa animazione*. Se l'opzione ☑ **Visualizza l'icona dell'area di notifica della barra delle applicazioni** è selezionata, gli utenti che lavorano su un computer remoto potranno vedere l'icona di Kaspersky Anti-Virus. L'icona dell'applicazione nell'area di notifica cambia in base all'operazione eseguita dall'applicazione. Per impostazione predefinita, l'icona dell'applicazione è animata. In questo caso, mostra solo lo stato di protezione del computer: se la protezione è abilitata, l'icona è colorata, mentre se la protezione è sospesa o disabilitata, l'icona diventa grigia.

- *Visualizza "Protected by Kaspersky Lab" nella schermata di accesso a Microsoft Windows*. Per impostazione predefinita, questo indicatore viene visualizzato nell'angolo superiore destro della schermata all'avvio di Kaspersky Anti-Virus e informa l'utente che il computer è protetto da qualsiasi tipo di minaccia.

  Se l'applicazione viene installata in un computer che utilizza Microsoft Windows Vista, questa opzione non è disponibile.

- *Visualizzazione dell'applicazione nel menu Start*. Se la casella **Visualizza Kaspersky Anti-Virus nel menu Start** è deselezionata, gli utenti che lavorano su un computer remoto non potranno vedere l'applicazione nel menu **Start**.

- *Visualizzazione nell'elenco dei programmi installati*. Se la casella **Visualizza Kaspersky Anti-Virus nell'elenco dei programmi installati** è deselezionata, gli utenti che lavorano su un computer remoto non potranno vedere l'applicazione nell'elenco dei programmi installati.

È inoltre possibile specificare gli stati dell'applicazione che non devono essere visualizzati nella finestra principale di Kaspersky Anti-Virus. Per questo scopo, cliccare sul pulsante **Impostazioni** nella sezione **Stati visualizzati nel computer client** e selezionare gli stati di protezione nella finestra che viene visualizzata. In questa stessa finestra è possibile specificare anche i periodi di monitoraggio dei database dell'applicazione.

In questa finestra è possibile modificare le informazioni relative all'assistenza tecnica presenti nella sezione **Info assistenza** della finestra **Supporto** di Kaspersky Anti-Virus in un computer remoto. Per aprire la finestra, cliccare sul pulsante **Impostazioni** nella sezione **Informazioni sull'assistenza personalizzata**.

Se è stato creato un criterio per l'applicazione (vedere pagina 225) che impedisce di modificare alcune impostazioni, non sarà possibile modificarle durante la configurazione dell'applicazione.

Per visualizzare e modificare le impostazioni avanzate dell'applicazione, eseguire le seguenti operazioni:

1. Aprire nella finestra delle proprietà del computer client (vedere pagina 212) la scheda **Applicazioni**.
2. Selezionare **Kaspersky Anti-Virus 6.0 per Windows Workstations MP4** nell'elenco delle applicazioni e cliccare sul pulsante **Proprietà**.
3. Nella scheda **Proprietà** della finestra dell'applicazione visualizzata selezionare la voce **Interazione con l'utente** nell'elenco a discesa e modificare le impostazioni.

GESTIONE DELLE ATTIVITÀ

In questa sezione sono incluse informazioni sulla gestione delle attività per Kaspersky Anti-Virus. Per maggiori dettagli sulla gestione delle attività tramite Kaspersky Administration Kit, consultare il manuale dell'amministratore per tale prodotto.

Durante l'installazione dell'applicazione viene creato un elenco di attività di sistema per ogni computer della rete. Questo elenco include attività di protezione (Anti-Virus File, Anti-Virus Web, Anti-Virus Posta, Difesa Proattiva, Anti-Spy, Anti-Hacker, Anti-Spam, Controllo Accessi), alcune attività di scansione anti-virus (Scansione Completa, Scansione Rapida) e attività di aggiornamento (aggiornamenti dei database e dei moduli dell'applicazione e rollback dei database).

È possibile gestire la pianificazione delle attività di sistema e modificare le relative impostazioni. Le attività di sistema non sono eliminabili.

È anche possibile creare attività personalizzate (vedere pagina 220), quali attività di scansione, aggiornamenti delle applicazioni e rollback degli aggiornamenti, e attività di installazione del file di chiave.

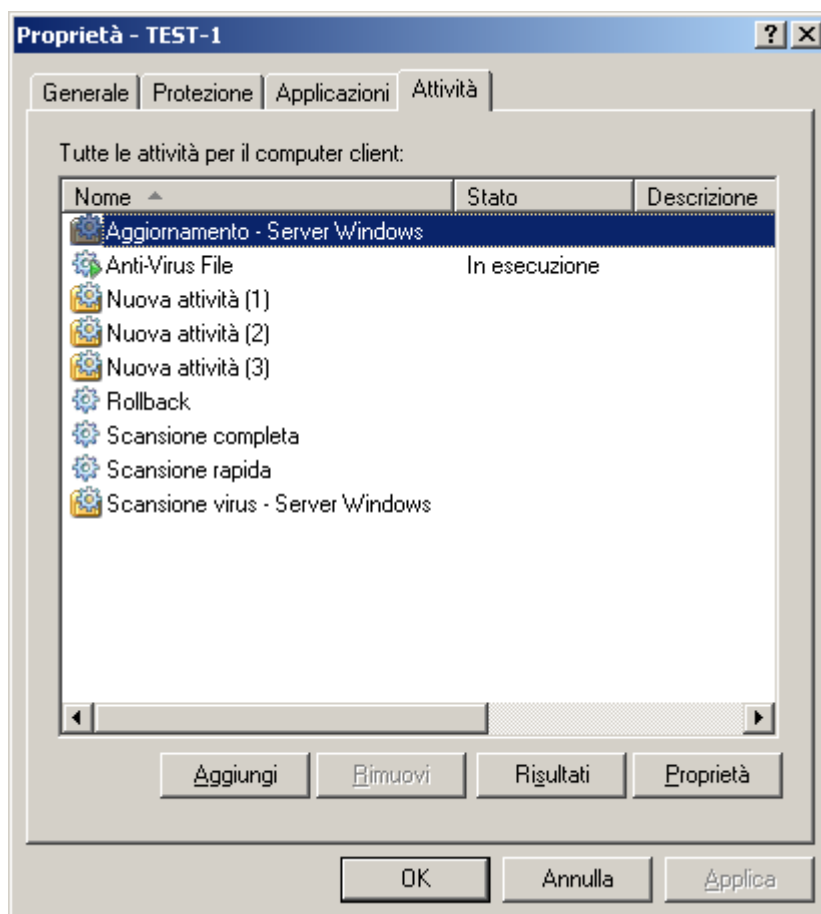



Fig. 17. Finestra delle proprietà del computer client. Scheda ***Attività***

➜ *Per aprire l'elenco di attività create per un computer client, eseguire le seguenti operazioni:*

1. Aprire Administration Console di Kaspersky Administration Kit.
2. Selezionare la cartella **Computer gestiti** con il nome del gruppo che include il computer client.
3. Nel gruppo selezionato, aprire la cartella **Computer client** e selezionare il computer per cui modificare le impostazioni dell'applicazione.
4. Selezionare il comando **Proprietà** dal menu di scelta rapida o la voce corrispondente nel menu **Azione** per aprire la finestra delle proprietà del computer client.
5. Nella finestra delle proprietà dell'applicazione che viene visualizzata, selezionare la scheda **Attività**. In questa scheda è possibile trovare l'elenco completo di attività create per il computer client.

AVVIO E ARRESTO DELLE ATTIVITÀ

Le attività vengono avviate nel computer client solo se è in esecuzione l'applicazione corrispondente (vedere pagina 213). Se l'applicazione viene chiusa, tutte le attività in esecuzione verranno terminate.

Le attività vengono avviate e arrestate automaticamente in base a una pianificazione o manualmente tramite i comandi del menu di scelta rapida e dalla finestra Visualizza impostazioni attività. È anche possibile sospendere e riprendere le attività.

Per avviare/arrestare/sospendere/riprendere manualmente un'attività, eseguire le seguenti operazioni:

1. Aprire nellafinestradelle proprietà del computer client (vedere a pag. 218) nella scheda **Attività**.
2. Selezionare l'attività richiesta e aprire il relativo menu di scelta rapida. Selezionare la voce **Avvia** per avviare l'attività oppure la voce **Termina** per terminarla. È inoltre possibile utilizzare le voci corrispondenti del menu **Azione**.

   Non è possibile sospendere e riprendere un'attività dal menu di scelta rapida.

   oppure

   Selezionare l'attività richiesta nell'elenco e cliccare sul pulsante **Proprietà**. È possibile utilizzare i bottoni della scheda **Generale** all'interno della finestra delle proprietà dell'attività per avviare, terminare, sospendere o riprendere un'attività.

CREAZIONE DI ATTIVITÀ

Quando si gestisce l'applicazione tramite Kaspersky Administration Kit, è possibile creare i seguenti tipi di attività:

- attività locali definite per singoli computer client;
- attività di gruppo definite per computer che appartengono a gruppi di amministrazione;
- attività per insiemi di computer definiti per computer esterni ai gruppi di amministrazione;
- le attività di Kaspersky Administration Kit sono specifiche per il server di aggiornamento: attività di download degli aggiornamenti, attività di backup e attività di invio rapporti.

Le attività di gruppo del computer vengono eseguite solo nell'insieme selezionato di computer. Se vengono aggiunti nuovi computer client a un gruppo contenente computer per cui è stata creata un'attività di installazione remota, l'attività non verrà eseguita per tali computer. È necessario creare una nuova attività o apportare le modifiche necessarie alle impostazioni dell'attività esistente.

È possibile eseguire le azioni seguenti in relazione alle attività:

- specificare le impostazioni delle attività;
- monitorare l'esecuzione dell'attività;
- copiare e spostare le attività da un gruppo all'altro, oppure eliminarle utilizzando i comandi standard **Copia/Incolla, Taglia/Incolla, Elimina** dal menu di scelta rapida oppure i comandi corrispondenti nel menu **Azione**;
- importare ed esportare le attività.

Per ulteriori informazioni sull'utilizzo delle attività, consultare il manuale di riferimento di Kaspersky Administration Kit.

Per creare un'attività locale, eseguire le seguenti operazioni:

1. Aprire la finestra delle proprietà del computer client (vedere pagina 218) nella scheda **Attività**.
2. Cliccare sul pulsante **Aggiungi**.
3. Verrà quindi avviata la Creazione guidata nuova attività (vedere pagina 221). Seguirne le istruzioni.

Per creare un'attività di gruppo, eseguire le seguenti operazioni:

1. Aprire Administration Console di Kaspersky Administration Kit.

2. Nella cartella **Computer gestiti**, aprire la cartella con il nome del gruppo richiesto.

3. Nel gruppo selezionato, aprire la cartella **Attività di gruppo** in cui è possibile trovare tutte le attività create per tale gruppo.

4. Aprire la Creazione guidata nuova attività cliccando sul collegamento **Crea nuova attività** nella barra delle applicazioni. Le specifiche per la creazione di attività di gruppo sono illustrate nel manuale di riferimento di Kaspersky Administration Kit.

Per creare un'attività per un gruppo di computer (un'attività di Kaspersky Administration Kit), eseguire le seguenti operazioni:

1. Aprire Administration Console di Kaspersky Administration Kit.

2. Selezionare la cartella **Attività per computer specifici** (**attività di Kaspersky Administration Kit**).

3. Aprire la Creazione guidata nuova attività cliccando sul collegamento **Crea nuova attività** nella barra delle applicazioni. Le specifiche per la creazione di attività di Kaspersky Administration Kit e di attività per gruppi di computer sono illustrate nel manuale di riferimento di Kaspersky Administration Kit.

CREAZIONE GUIDATA ATTIVITÀ LOCALE

Creazione guidata attività locale viene avviato quando si selezionano i comandi corrispondenti dal menu di scelta rapida per il computer client o nella finestra delle proprietà per tale computer.

La procedura guidata è costituita da una serie di finestre (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Indietro** ed **Avanti**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per annullare la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

PASSAGGIO 1. IMMISSIONE DI DATI GENERALI NELL'ATTIVITÀ

La prima finestra della procedura guidata è introduttiva e richiede solo l'immissione del nome dell'attività nel campo **Nome**.

PASSAGGIO 2. SELEZIONE DI UN'APPLICAZIONE E DI UN TIPO DI ATTIVITÀ

In questo passaggio è necessario specificare l'applicazione per cui si intende creare l'attività (Kaspersky Anti-Virus 6.0 per Windows Workstations MP4 o Administration Agent). È necessario selezionare anche il tipo di attività. Le attività disponibili per Kaspersky Anti-Virus 6.0 sono:

- *File dei virus*: attività di scansione anti-virus delle aree specificate dall'utente.
- *Aggiornamento*: consente di recuperare e implementare pacchetti di aggiornamento per l'applicazione.
- *Aggiorna rollback*: esegue il rollback all'ultimo aggiornamento dell'applicazione.
- *Installazione file di chiave*: installazione di un file di chiave per una nuova licenza, se necessario per utilizzare l'applicazione.

PASSAGGIO 3. CONFIGURAZIONE DEL TIPO DI ATTIVITÀ SELEZIONATO

Il contenuto della finestra delle impostazioni varia in base al tipo di attività selezionato.

Le attività di scansione anti-virus richiedono di specificare l'azione che Kaspersky Anti-Virus eseguirà se rileva un oggetto dannoso (vedere pagina 127) e di creare un elenco di oggetti da sottoporre a scansione (vedere pagina 126).

Per le attività di aggiornamento del database e dei moduli dell'applicazione, è necessario specificare l'origine che verrà utilizzata per scaricare gli aggiornamenti (vedere pagina 137). L'origine di aggiornamento predefinita è il server di aggiornamento di Kaspersky Administration Kit.

Le attività di rollback degli aggiornamenti non presentano impostazioni specifiche.

Per le attività di installazione della chiave di licenza, specificare il percorso del file di chiave mediante il pulsante **Sfoglia**. Per aggiungere un file come chiave di licenza per una licenza aggiuntiva, selezionare la casella corrispondente. La chiave di licenza aggiuntiva verrà attivata alla scadenza della chiave di licenza già attiva.

Nel campo seguente sono visualizzare informazioni sulla licenza specifica (numero, tipo e data di scadenza della licenza).

PASSAGGIO 4. CONFIGURAZIONE DI UNA PIANIFICAZIONE

Dopo aver configurato le attività, viene offerta la possibilità di configurare la pianificazione di esecuzione automatica dell'attività.

A tale scopo, selezionare la frequenza di esecuzione dell'attività dal menu a discesa nella finestra delle impostazioni di pianificazione e modificare tali impostazioni nella parte inferiore della finestra.

PASSAGGIO 5. COMPLETAMENTO DELLA CREAZIONE DELL'ATTIVITÀ

Nell'ultima finestra della procedura guidata viene indicato che la creazione dell'attività è stata completata.

CONFIGURAZIONE DELLE ATTIVITÀ

La configurazione delle attività dell'applicazione tramite l'interfaccia di Kaspersky Administration Kit è simile alla stessa procedura eseguita tramite l'interfaccia locale di Kaspersky Anti-Virus, con la differenza che le impostazioni vengono modificate singolarmente per ogni utente, ad esempio la pianificazione dell'esecuzione delle attività di scansione o le impostazioni specifiche di Kaspersky Administration Kit, quali le impostazioni che consentono/bloccano la gestione delle attività di scansione locale eseguite dagli utenti.

Se è stato creato un criterio per l'applicazione (vedere pagina 225) che impedisce di modificare alcune impostazioni, non sarà possibile modificarle durante la configurazione dell'applicazione.

All the tabs, except for the **Properties** tab (see figure below), are standard for the Kaspersky Administration Kit application and are covered more in detail in the Reference Guide. La scheda **Proprietà** contiene impostazioni specifiche per Kaspersky Anti-Virus. Il contenuto di questa scheda varia in base al tipo di attività selezionato.

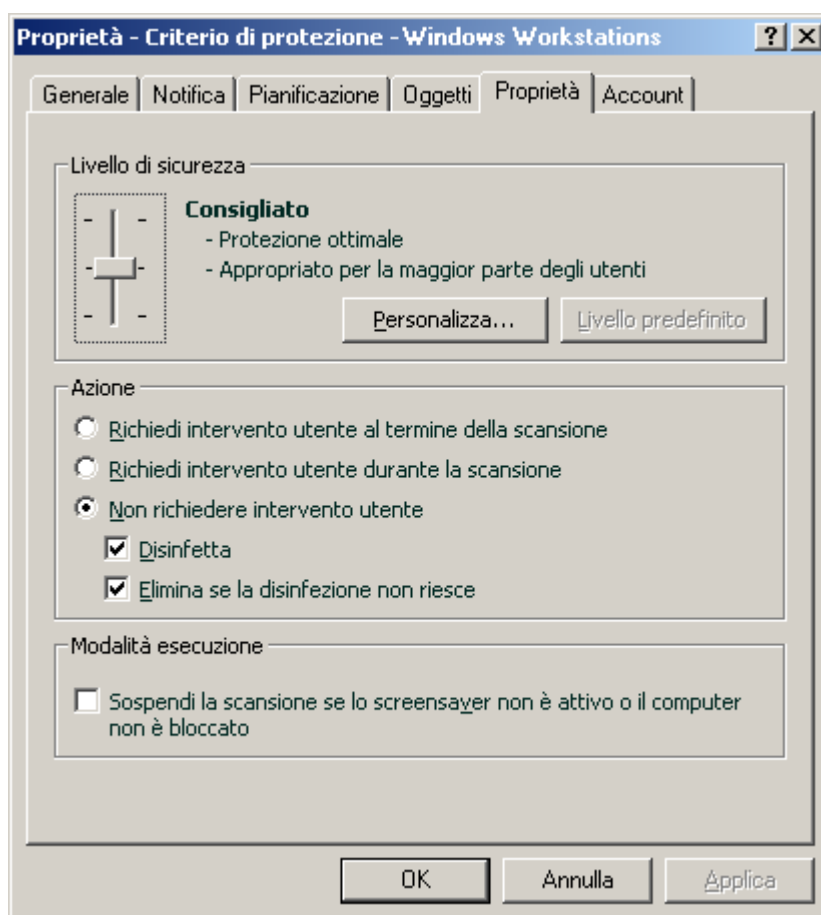



Fig. 18. Finestra delle proprietà dell'attività. Scheda ***Proprietà***

Per visualizzare e modificare le attività locali, eseguire le seguenti operazioni:

1. Aprire nella finestra delle proprietà del computer client (vedere pagina 218) la scheda **Attività**.
2. Selezionare un'attività nell'elenco e cliccare sul pulsante **Proprietà**. Verrà aperta la finestra delle impostazioni dell'attività.

Per visualizzare le attività di gruppo, eseguire le seguenti operazioni:

1. Aprire Administration Console di Kaspersky Administration Kit.
2. Nella cartella **Computer gestiti**, aprire la cartella con il nome del gruppo richiesto.
3. Nel gruppo selezionato, aprire la cartella **Attività di gruppo** in cui è possibile trovare tutte le attività create per tale gruppo.
4. Selezionare l'attività richiesta dalla struttura ad albero della console per visualizzarne e modificarne le proprietà.

   Nella barra delle applicazioni verranno visualizzate informazioni complete sull'attività, insieme ai collegamenti per gestire l'esecuzione dell'attività e la modifica delle relative impostazioni. Le specifiche per la creazione di attività di gruppo sono illustrate nel manuale di riferimento di Kaspersky Administration Kit.

Per visualizzare attività per un gruppo di computer (un'attività di Kaspersky Administration Kit), eseguire le seguenti operazioni:

1. Aprire Administration Console di Kaspersky Administration Kit.
2. Selezionare la cartella **Attività per computer specifici** (**Attività di Kaspersky Administration Kit**).
3. Selezionare l'attività richiesta dalla struttura ad albero della console per visualizzarne e modificarne le proprietà.

   Nella barra delle applicazioni verranno visualizzate informazioni complete sull'attività, insieme ai collegamenti per gestire l'esecuzione dell'attività e la modifica delle relative impostazioni. Le specifiche delle attività di Kaspersky Administration Kit e le attività per gruppi di computer sono illustrate nel manuale di riferimento di Kaspersky Administration Kit.

GESTIONE DEI CRITERI

L'impostazione di criteri consente di applicare impostazioni universali dell'applicazione e dell'attività ai computer client che appartengono a un singolo gruppo di amministrazione.

In questa sezione sono incluse informazioni sulla creazione e configurazione dei criteri per Kaspersky Anti-Virus 6.0 per Windows Workstations MP4. Per ulteriori informazioni sui concetti legati alla gestione dei criteri tramite Kaspersky Administration Kit, consultare il manuale dell'amministratore per l'applicazione.

Quando si crea e si configura un criterio, è possibile bloccare completamente o in parte la modifica delle impostazioni nei criteri per i gruppi nidificati, le impostazioni delle attività e le impostazioni delle applicazioni. A tale scopo, premere il pulsante . Dovrebbe diventare per le impostazioni bloccate.

Per aprire l'elenco di criteri per Kaspersky Anti-Virus, eseguire le seguenti operazioni:

1. Aprire Administration Console diKaspersky Administration Kit.
2. Selezionare la cartella **Computer gestiti** con il nome del gruppo che include il computer client.
3. Nel gruppo selezionato, aprire la cartella **Criteri** in cui è possibile trovare tutti i criteri creati per tale gruppo.

CREAZIONE DI CRITERI

Quando si utilizza Kaspersky Anti-Virus tramite Kaspersky Administration Kit, è possibile creare i seguenti tipi di criteri:

È possibile eseguire le azioni seguenti in relazione ai criteri:

- configurare i criteri;
- copiare e spostare i criteri da un gruppo all'altro, oppure eliminarli utilizzando i comandi standard **Copia/Incolla, Taglia/Incolla, Elimina** dal menu di scelta rapida oppure i comandi corrispondenti nel menu **Azione**;
- importare ed esportare le impostazioni dei criteri.

La gestione dei criteri è illustrata in maggior dettagli nel manuale di riferimento di Kaspersky Administration Kit.

Per creare un criterio, eseguire le seguenti operazioni:

1. Aprire Administration Console di Kaspersky Administration Kit.
2. Nella cartella **Computer gestiti**, aprire la cartella con il nome del gruppo richiesto.
3. Nel gruppo selezionato, aprire la cartella **Criteri** in cui è possibile trovare tutti i criteri creati per tale gruppo.

4. Aprire la Creazione guidata nuova attività cliccando sul collegamento **Crea nuovo criterio** nella barra delle applicazioni.

5. Verrà quindi avviata la Creazione guidata nuova attività nella finestra visualizzata (vedere a pag. 225) di cui sarà necessario seguire le indicazioni.

CREAZIONE GUIDATA CRITERIO

È possibile avviare Creazione guidata criterio selezionando l'azione corrispondente dal menu di scelta rapida della cartella **Criteri** del gruppo di amministrazione selezionato oppure cliccando sul collegamento nel riquadro dei risultati (per le cartelle **Criteri**).

La procedura guidata è costituita da una serie di finestre (passaggi) tra le quali è possibile spostarsi servendosi dei pulsanti **Indietro** ed **Avanti**. Per chiudere la procedura guidata al completamento, utilizzare il pulsante **Fine**. Per annullare la procedura in qualsiasi momento, utilizzare il pulsante **Annulla**.

PASSAGGIO 1. IMMISSIONE DI DATI GENERALI NEL CRITERIO

Le prime finestre della procedura guidata sono introduttive. In queste finestre è necessario specificare il nome del criterio nel campo **Nome** e selezionare **Kaspersky Anti-Virus 6.0 per Windows Workstations MP4** nel menu a discesa **Nome applicazione**.

Se si esegue la Creazione guidata criterio dal nodo **Criteri** della barra delle applicazioni (utilizzando **Crea nuovo criterio di Kaspersky Anti-Virus for Windows Workstations MP4**), non sarà possibile selezionare un'applicazione.

Se si desidera creare un criterio basato sulle impostazioni di un criterio esistente creato per la versione precedente dell'applicazione, selezionare la casella **Utilizza impostazioni del criterio esistente** e il criterio di cui si desidera utilizzare le impostazioni per il nuovo criterio. Per selezionare un criterio, cliccare sul pulsante **Seleziona** che aprirà l'elenco dei criteri esistenti che possono essere utilizzati per crearne uno nuovo.

PASSAGGIO 2. SELEZIONE DELLO STATO DEL CRITERIO

In questa finestra è possibile specificare lo stato del criterio creato, selezionando una delle opzioni seguenti: criterio attivo, criterio inattivo o criterio utente mobile. Per ulteriori informazioni sullo stato dei criteri, consultare il manuale di riferimento di Kaspersky Administration Kit.

È possibile creare vari criteri per una singola applicazione in un gruppo, ma solo uno di essi può essere il criterio attivo.

PASSAGGIO 3. IMPORTAZIONE DELLE IMPOSTAZIONI DELL'APPLICAZIONE

Se si dispone di un file con impostazioni dell'applicazione salvate in precedenza, è possibile specificarne il percorso utilizzando il pulsante **Importa**. Nelle finestre della procedura guidata visualizzate da quel momento in poi verranno mostrate le impostazioni importate.

PASSAGGIO 4. CONFIGURAZIONE DELLA PROTEZIONE

In questo passaggio è possibile abilitare/disabilitare o configurare i componenti di protezione che verranno utilizzati nel criterio.

Per impostazione predefinita, tutti i componenti di protezione sono abilitati. Per disabilitare singoli componenti, deselezionare la casella accanto ad essi. Per modificare un componente di protezione, selezionarlo nell'elenco e cliccare sul pulsante **Configura**.

PASSAGGIO 5. CONFIGURAZIONE DELLA PROTEZIONE TRAMITE PASSWORD

In questa finestra della procedura guidata (vedere la figura seguente) è possibile modificare le impostazioni generali dell'applicazione: abilitare/disabilitare Auto-Difesa, abilitare/disabilitare il controllo esterno dei servizi di sistema, impostare o rimuovere la protezione tramite password per l'applicazione.

PASSAGGIO 6. CONFIGURAZIONE DELL'AREA ATTENDIBILE

In questa finestra della procedura guidata è possibile configurare l'area attendibile, ovvero aggiungere il software utilizzato per l'amministrazione della rete all'elenco di applicazioni attendibili ed escludere vari tipi di file dalla scansione.

PASSAGGIO 7. CONFIGURAZIONE DELL'INTERAZIONE CON L'UTENTE

In questo passaggio è possibile specificare le impostazioni per l'interazione dell'utente con Kaspersky Anti-Virus:

- visualizzazione dell'interfaccia dell'applicazione in un computer remoto;
- invio di notifiche degli eventi agli utenti;
- visualizzazione dell'icona dell'applicazione nell'area di notifica della barra delle applicazioni e della relativa animazione;
- visualizzazione di "Protected by Kaspersky Lab" nella schermata di accesso a Microsoft Windows;
- visualizzazione dell'applicazione nel menu Start;
- visualizzazione dell'applicazione nell'elenco dei programmi installati.

PASSAGGIO 8. COMPLETAMENTO DELLA CREAZIONE DEL CRITERIO

Nell'ultima finestra della procedura guidata viene indicato che la creazione del criterio è stata completata.

Al termine della procedura guidata, il criterio per l'applicazione verrà aggiunto alla cartella **Criteri** del gruppo corrispondente, diventando visibile nella struttura ad albero della console.

È possibile modificare le impostazioni del criterio creato e impostare restrizioni alla modifica delle relative impostazioni utilizzando i bottoni e per ogni gruppo di impostazioni. Se viene visualizzata l'icona , l'utente del computer client non potrà modificare le impostazioni. Se viene visualizzata l'icona , l'utente del computer client potrà modificare le impostazioni. Il criterio verrà applicato ai computer client durante la prima sincronizzazione dei client con il server.

CONFIGURAZIONE DEL CRITERIO

Durante la fase di modifica è possibile modificare il criterio e bloccare la modifica delle impostazioni nei criteri dei gruppi nidificati e nelle impostazioni dell'applicazione e dell'attività. Le impostazioni del criterio possono essere modificate nella finestra delle proprietà del criterio (vedere la figura seguente).

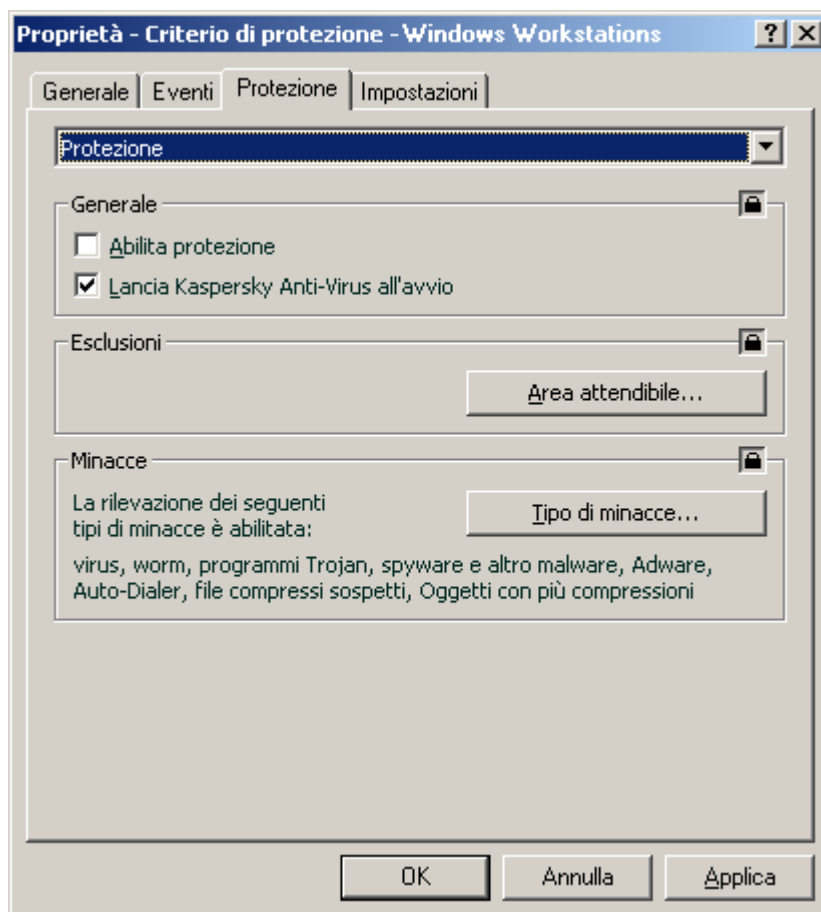



Fig. 18. Finestra delle proprietà dei criteri. Scheda ***Protezione***

Tutte le schede, ad eccezione delle schede **Protezione** e **Impostazioni**, sono standard per Kaspersky Administration Kit e sono descritte in maggior dettaglio nel manuale dell'amministratore.

Le impostazioni dei criteri per Kaspersky Anti-Virus 6.0 includono le impostazioni dell'applicazione (vedere pagina 215) e le impostazioni dell'attività (vedere pagina 222). Nella scheda **Impostazioni** vengono visualizzate le impostazioni dell'applicazione e nella scheda **Protezione** le impostazioni dell'attività.

Per modificare le impostazioni, selezionare il valore richiesto nel menu a discesa nella parte superiore della finestra e impostarlo.

Per visualizzare e modificare le impostazioni dei criteri, eseguire le seguenti operazioni:

1. Aprire Administration Console di Kaspersky Administration Kit.
2. Nella cartella **Computer gestiti**, aprire la cartella con il nome del gruppo richiesto.
3. Nel gruppo selezionato, aprire la cartella **Criteri** in cui è possibile trovare tutti i criteri creati per tale gruppo.
4. Selezionare il criterio richiesto dalla struttura ad albero della console per visualizzarne e modificarne le proprietà.

5. Nella barra delle applicazioni verranno visualizzate informazioni complete sul criterio, insieme ai collegamenti per gestire lo stato del criterio e la modifica delle relative impostazioni.

   oppure

   Aprire il menu di scelta rapida per il criterio selezionato e utilizzare l'elemento **Proprietà** per aprire la finestra delle impostazioni dei criteri di Kaspersky Anti-Virus.

   Le specifiche dell'utilizzo dei criteri sono disponibili nel manuale di riferimento di Kaspersky Administration Kit.

UTILIZZO DI CODICE DI TERZE PARTI

Durante lo sviluppo di Kaspersky Anti-Virus, è stato utilizzato codice di terze parti.

IN QUESTA SEZIONE

Libreria Boost 1.30 230

Libreria LZMA SDK 4.40, 4.43 230

Libreria Windows Template (WTL 7.5) 230

Libreria Windows Installer XML (WiX-2.0) 231

Libreria ZIP-2.31 234

Libreria ZLIB-1.0.4, ZLIB-1.1.3, ZLIB-1.2.3 235

Libreria UNZIP-5.51 235

Libreria LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12 236

Libreria LIBJPEG-6B 238

Libreria LIBUNGIF-4.1.4 239

Libreria MD5 MESSAGE-DIGEST ALGORITHM-REV. 2 239

Libreria MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004 239

Libreria INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999 240

Libreria CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004 240

Libreria COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum 240

Libreria PLATFORM INDEPENDENT IMAGE CLASS 241

Libreria FLEX PARSER (FLEXLEXER)-V. 1993 241

Libreria ENSURECLEANUP, SWMRG, LAYOUT-V. 2000 241

Libreria STDSTRING- V. 1999 242

Libreria T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006 242

Libreria NTSERVICE- V. 1997 243

Libreria SHA-1-1.2 243

Libreria COCOA SAMPLE CODE- V. 18.07.2007 243

Libreria PUTTY SOURCES-25.09.2008 244

Altre informazioni 245

LIBRERIA BOOST 1.30

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Boost 1.30. Copyright (C) 2003, Christof Meerwald.

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the

Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBRERIA LZMA SDK 4.40, 4.43

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria LZMA SDK 4.40, 4.43. Copyright (C) 1999-2006, Igor Pavlov.

LIBRERIA WINDOWS TEMPLATE (WTL 7.5)

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Windows Template 7.5. Copyright (C) 2006, Microsoft Corporation.

Microsoft Public License (Ms-PL)

Published: October 12, 2006

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. **Definizioni**

   The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

   A "contribution" is the original software, or any additions or changes to the software.

   A "contributor" is any person that distributes its contribution under this license.

   "Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. **Grant of Rights**

   (A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. **Conditions and Limitations**

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

LIBRERIA WINDOWS INSTALLER XML (WIX-2.0)

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Windows Installer XML (WiX). Copyright (C) 2009, Microsoft Corporation.

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.

1. **DEFINITIONS**

"Contribution" means:

f. in the case of the initial Contributor, the initial code and documentation distributed under this Agreement, and

g. in the case of each subsequent Contributor:

i) changes to the Program, and

ii) additions to the Program;

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. **GRANT OF RIGHTS**

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. **REQUIREMENTS**

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably allows subsequent Recipients to identify the originator of the Contribution.

4. **COMMERCIAL DISTRIBUTION**

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5. **NO WARRANTY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. **DISCLAIMER OF LIABILITY**

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. **GENERAL**

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

LIBRERIA ZIP-2.31

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria ZIP-2.31. Copyright (C) 1990-2005, Info-ZIP.

This is version 2005-Feb-10 of the Info-ZIP copyright and license.

The definitive version of this document should be available at ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely.

Copyright (c) 1990-2005 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

LIBRERIA ZLIB-1.0.4, ZLIB-1.1.3, ZLIB-1.2.3

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria ZLIB-1.0.4, ZLIB-1.1.3, ZLIB-1.2.3. Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

LIBRERIA UNZIP-5.51

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria UNZIP-5.51. Copyright (c) 1990-2004 Info-ZIP.

This is version 2004-May-22 of the Info-ZIP copyright and license.

The definitive version of this document should be available at ftp://ftp.info-zip.org/pub/infozip/license.html indefinitely.

Copyright (c) 1990-2004 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Christian Spieler, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.

2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.

3. Altered versions--including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions--must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being

Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

LIBRERIA LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria LIBPNG-1.0.1, LIBPNG-1.2.8, LIBPNG-1.2.12.

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright (c) 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, "Contributing Authors" is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied "AS IS". The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.
2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.
3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A "png_get_copyright" function is available, for convenient use in "about" boxes and the like:

printf("%s",png_get_copyright(NULL));

Also, the PNG logo (in PNG format, of course) is supplied in the files "pngbar.png" and "pngbar.jpg (88x31) and "pngnow.png" (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a certification mark of the Open Source Initiative.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

August 13, 2009

LIBRERIA LIBJPEG-6B

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria LIBJPEG-6B. Copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

LEGAL ISSUES

============

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-2009, Thomas G. Lane, Guido Vollbeding.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this

README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch,

sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA.

ansi2knr.c is NOT covered by the above copyright and conditions, but instead

by the usual distribution terms of the Free Software Foundation; principally,

that you must include source code if you redistribute it. (See the file

ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part

of any program generated from the IJG code, this does not limit you more than

the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf.

It is copyright by the Free Software Foundation but is freely distributable.

The same holds for its supporting scripts (config.guess, config.sub, ltmain.sh). Another support script, install-sh, is copyright by X Consortium but is also freely distributable.

The IJG distribution formerly included code to read and write GIF files.

To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that

> "The Graphics Interchange Format(c) is the Copyright property of
>
> CompuServe Incorporated. GIF(sm) is a Service Mark property of
>
> CompuServe Incorporated."

LIBRERIA LIBUNGIF-4.1.4

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria LIBUNGIF-4.1.4. Copyright (C) 1997, Eric S. Raymond.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

LIBRERIA MD5 MESSAGE-DIGEST ALGORITHM-REV. 2

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria MD5 MESSAGE-DIGEST ALGORITHM-REV. 2.

LIBRERIA MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria MD5 MESSAGE-DIGEST ALGORITHM-V. 18.11.2004.

LIBRERIA INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria INDEPENDENT IMPLEMENTATION OF MD5 (RFC 1321)-V. 04.11.1999. Copyright (C) 1991-2, RSA Data Security, Inc.

RSA's MD5 disclaimer

LIBRERIA CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria CONVERSION ROUTINES BETWEEN UTF32, UTF-16, AND UTF-8-V. 02.11.2004. Copyright 2001-2004 Unicode, Inc.

Disclaimer

Limitations on Rights to Redistribute This Code

LIBRERIA COOL OWNER DRAWN MENUS-V. 2.4, 2.63 BY BRENT CORKUM

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria COOL OWNER DRAWN MENUS-V. 2.4, 2.63 By Brent Corkum.

You are free to use/modify this code but leave this header intact. This class is public domain so you are free to use it any of your applications (Freeware,Shareware,Commercial). All I ask is that you let me know so that if you have a real winner I can brag to my buddies that some of my code is in your app. I also wouldn't mind if you sent me a copy of your application since I like to play with new stuff.

Brent Corkum, corkum@rocscience.com

LIBRERIA PLATFORM INDEPENDENT IMAGE CLASS

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria PLATFORM INDEPENDENT IMAGE CLASS. Copyright (C) 1995, Alejandro Aguilar Sierra (asierra@servidor.unam.mx).

Covered code is provided under this license on an "as is" basis, without warranty of any kind, either expressed or implied, including, without limitation, warranties that the covered code is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the covered code is with you. Should any covered code prove defective in any respect, you (not the initial developer or any other contributor) assume the cost of any necessary servicing, repair or correction. This disclaimer of warranty constitutes an essential part of this license. No use of any covered code is authorized hereunder except under this disclaimer.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, including commercial applications, freely and without fee, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

LIBRERIA FLEX PARSER (FLEXLEXER)-V. 1993

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria FLEX PARSER (FLEXLEXER)-V. 1993. Copyright (c) 1993 The Regents of the University of California.

This code is derived from software contributed to Berkeley by Kent Williams and Tom Epperly.

Redistribution and use in source and binary forms with or without modification are permitted provided that: (1) source distributions retain this entire copyright notice and comment, and (2) distributions including binaries display the following acknowledgement: ``This product includes software developed by the University of California, Berkeley and its contributors'' in the documentation or other materials provided with the distribution and in all advertising materials mentioning features or use of this software. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This file defines FlexLexer, an abstract class which specifies the external interface provided to flex C++ lexer objects, and yyFlexLexer, which defines a particular lexer class.

LIBRERIA ENSURECLEANUP, SWMRG, LAYOUT-V. 2000

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria ENSURECLEANUP, SWMRG, LAYOUT-V. 2000. Copyright (C) 2009, Microsoft Corporation.

NOTICE SPECIFIC TO SOFTWARE AVAILABLE ON THIS WEB SITE.

All Software is the copyrighted work of Microsoft and/or its suppliers. Use of the Software is governed by the terms of the end user license agreement, if any, which accompanies or is included with the Software ("License Agreement").

If Microsoft makes Software available on this Web Site without a License Agreement, you may use such Software to design, develop and test your programs to run on Microsoft products and services.

If Microsoft makes any code marked as "sample" available on this Web Site without a License Agreement, then that code is licensed to you under the terms of the Microsoft Limited Public License http://msdn.microsoft.com/en-us/cc300389.aspx#MLPL.

The Software is made available for download solely for use by end users according to the License Agreement or these TOU. Any reproduction or redistribution of the Software not in accordance with the License Agreement or these TOU is expressly prohibited.

WITHOUT LIMITING THE FOREGOING, COPYING OR REPRODUCTION OF THE SOFTWARE TO ANY OTHER SERVER OR LOCATION FOR FURTHER REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PROHIBITED, UNLESS SUCH REPRODUCTION OR REDISTRIBUTION IS EXPRESSLY PERMITTED BY THE LICENSE AGREEMENT ACCOMPANYING SUCH SOFTWARE.

FOR YOUR CONVENIENCE, MICROSOFT MAY MAKE AVAILABLE ON THIS WEB SITE, TOOLS AND UTILITIES FOR USE AND/OR DOWNLOAD. MICROSOFT DOES NOT MAKE ANY ASSURANCES WITH REGARD TO THE ACCURACY OF THE RESULTS OR OUTPUT THAT DERIVES FROM SUCH USE OF ANY SUCH TOOLS AND UTILITIES. PLEASE RESPECT THE INTELLECTUAL PROPERTY RIGHTS OF OTHERS WHEN USING THE TOOLS AND UTILITIES MADE AVAILABLE ON THIS WEB SITE.

RESTRICTED RIGHTS LEGEND. Any Software which is downloaded from the Web Site for or on behalf of the United States of America, its agencies and/or instrumentalities ("U.S. Government"), is provided with Restricted Rights. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19, as applicable. Manufacturer is Microsoft Corporation, One Microsoft Way, Redmond, WA 98052-6399.

LIBRERIA STDSTRING- V. 1999

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria STDSTRING- V. 1999. Copyright (C) 1999, Joseph M. O'Leary.

This code is free. Use it anywhere you want.

Rewrite it, restructure it, whatever. Please don't blame me if it makes your $30 billion dollar satellite explode in orbit. If you redistribute it in any form, I'd appreciate it if you would leave this notice here.

LIBRERIA T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria T-REX (TINY REGULAR EXPRESSION LIBRARY)- V. 2003-2006. Copyright (C) 2003-2006, Alberto Demichelis.

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

LIBRERIA NTSERVICE- V. 1997

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria NTSERVICE- V. 1997. Copyright (C) 1997 by Joerg Koenig and the ADG mbH, Mannheim, Germany.

Distribute freely, except: don't remove my name from the source or documentation (don't take credit for my work), mark your changes (don't get me blamed for your possible bugs), don't alter or remove this notice.

No warrantee of any kind, express or implied, is included with this software; use at your own risk, responsibility for damages (if any) to anyone resulting from the use of this software rests entirely with the user.

Send bug reports, bug fixes, enhancements, requests, flames, etc., and I'll try to keep a version up to date. I can be reached as follows:

J.Koenig@adg.de (company site)

Joerg.Koenig@rhein-neckar.de (private site)

MODIFIED BY TODD C. WILSON FOR THE ROAD RUNNER NT LOGIN SERVICE.

HOWEVER, THESE MODIFICATIONS ARE BROADER IN SCOPE AND USAGE AND CAN BE USED IN OTHER PROJECTS WITH NO CHANGES.

MODIFIED LINES FLAGGED/BRACKETED BY "//!! TCW MOD"

LIBRERIA SHA-1-1.2

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria SHA-1-1.2. Copyright (C) 2001, The Internet Society.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

LIBRERIA COCOA SAMPLE CODE- V. 18.07.2007

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria Cocoa sample code- v. Copyright (C) 2007, Apple Inc.

Disclaimer: IMPORTANT: This Apple software is supplied to you by Apple Inc. ("Apple")

in consideration of your agreement to the following terms, and your use, installation, modification or redistribution of this Apple software constitutes acceptance of these terms. If you do not agree with these terms, please do not use, install, modify or redistribute this Apple software.

In consideration of your agreement to abide by the following terms, and subject to these terms, Apple grants you a personal, non – exclusive license, under Apple's copyrights in this original Apple software (the "Apple Software"), to use, reproduce, modify and redistribute the Apple Software, with or without modifications, in source and / or binary forms; provided that if you redistribute the Apple Software in its entirety and without modifications, you must retain this notice and the following text and disclaimers in all such redistributions of the Apple Software. Neither the name, trademarks, service marks or logos of Apple Inc. may be used to endorse or promote products derived from the Apple Software without specific prior written permission from Apple. Except as expressly stated in this notice, no other rights or licenses, express or implied, are granted by Apple herein, including but not limited to any patent rights that may be infringed by your derivative works or by other works in which the Apple Software may be incorporated.

The Apple Software is provided by Apple on an "AS IS" basis.

APPLE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NON - INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE APPLE SOFTWARE OR ITS USE AND OPERATION ALONE OR IN COMBINATION WITH YOUR PRODUCTS.

IN NO EVENT SHALL APPLE BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) ARISING IN ANY WAY OUT OF THE USE, REPRODUCTION, MODIFICATION AND / OR DISTRIBUTION OF THE APPLE SOFTWARE, HOWEVER CAUSED AND WHETHER UNDER THEORY OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

LIBRERIA PUTTY SOURCES-25.09.2008

Durante lo sviluppo dell'applicazione è stata utilizzata la libreria PUTTY SOURCES-25.09.2008. Copyright (C) 1997-2009, Simon Tatham.

The PuTTY executables and source code are distributed under the MIT licence, which is similar in effect to the BSD licence. (This licence is Open Source certified http://www.opensource.org/licenses/ and complies with the Debian Free Software Guidelines http://www.debian.org/social_contract)

The precise licence text, as given in the About box and in the file LICENCE in the source distribution, is as follows:

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, Ben Harris, Malcolm Smith, Ahmad Khalifa, Markus Kuhn, Colin Watson, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SIMON TATHAM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

In particular, anybody (even companies) can use PuTTY without restriction (even for commercial purposes) and owe nothing to me or anybody else. Also, apart from having to maintain the copyright notice and the licence text in derivative products, anybody (even companies) can adapt the PuTTY source code into their own programs and products (even commercial products) and owe nothing to me or anybody else. And, of course, there is no warranty and if PuTTY causes you damage you're on your own, so don't use it if you're unhappy with that.

In particular, note that the MIT licence is compatible with the GNU GPL. So if you want to incorporate PuTTY or pieces of PuTTY into a GPL program, there's no problem with that.

ALTRE INFORMAZIONI

The Software may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar free software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code (Open Source Software). If such licenses require that for any software, which is distributed to someone in an executable binary format, that the source code also be made available to those users, then the source code should be made available by sending the request to source@kaspersky.com.

GLOSSARIO

A

Administration agent

Componente di Kaspersky Administration Kit che gestisce le interazioni tra Administration Server e le applicazioni Kaspersky Lab installate su uno specifico nodo di rete (una workstation o un server). Questo componente è lo stesso per tutte le applicazioni Windows nella linea di prodotti. Esistono versioni diverse di Administration agent per Novell- e Unix-specifiche prodotte da Kaspersky Lab.

Aggiornamenti critici

Aggiornamenti critici ai moduli dell'applicazione Kaspersky Lab.

Aggiornamenti del database

Elenco di indirizzi Web, definiti come phishing dagli specialisti di Kaspersky Lab. I database vengono scaricati dai server degli aggiornamenti di Kaspersky Lab nel computer e collegati automaticamente all'applicazione.

Aggiornamenti disponibili

Gruppo di aggiornamenti per i moduli dell'applicazione Kaspersky Lab, inclusi gli aggiornamenti critici accumulati in un periodo di tempo e le modifiche apportate all'architettura dell'applicazione.

Aggiornamento

Procedura di sostituzione/aggiunta di nuovi file (database o moduli dell'applicazione) recuperati dai server degli aggiornamenti di Kaspersky Lab.

Amministratore di Kaspersky Anti-Virus

La persona che gestisce le operazioni dell'applicazione attraverso il sistema di amministrazione remota centralizzata di Kaspersky Anti-Virus.

Analisi euristica

Tecnologia di rilevamento delle minacce che non possono essere identificate dai database Anti-Virus. Consente di rilevare gli oggetti sospettati di essere stati colpiti da un virus sconosciuto o da una variante nuova di virus noti.

L'utilizzo dell'analisi euristica consente di rilevare fino al 92% delle minacce. Questo meccanismo è estremamente efficace e determina falsi positivi molto raramente.

I file rilevati dall'analisi euristica sono considerati sospetti.

Applicazione non compatibile

Applicazione anti-virus di uno sviluppatore di terze parti o applicazione Kaspersky Lab che non supporta la gestione attraverso Kaspersky Administration Kit.

Archivio

File "contenente" uno o diversi altri oggetti che possono anche essere archivi.

Attacco di virus

Serie di attacchi intenzionali per infettare un computer con un virus.

Backup

Memoria speciale destinata al salvataggio delle copie di backup di oggetti creati prima della disinfezione o eliminazione iniziale.

BLACK LIST DI INDIRIZZI

Elenco di indirizzi di posta elettronica che inviano i messaggi che dovrebbero essere bloccati da parte dell'applicazione Kaspersky Lab, indipendentemente dal contenuto.

BLACKLIST DEI FILE CHIAVE

Modello in base al quale viene generata una notifica di minaccia di attacco di virus. Un elenco di file chiave bloccati è necessario per il funzionamento delle applicazioni di Kaspersky Lab. Il contenuto del file viene aggiornato insieme ai database.

BLOCCO DELL'OGGETTO

Negazione dell'accesso a un oggetto da parte di applicazioni esterne. Un oggetto bloccato non può essere letto, eseguito, modificato o eliminato.

C

CARTELLA DI DATI

La cartella contenente le cartelle e i database del servizio necessari per utilizzare l'applicazione. Se la cartella di dati viene spostata, tutte le informazioni in essa incluse devono essere salvate nella nuova posizione.

CLIENT

Il programma che si connette con il server utilizzando un servizio specifico. Ad esempio, Netscape è un client WWW e stabilisce la connessione con i server Web per scaricare pagine Web.

COPIA DI BACKUP

Creazione di una copia di backup di un file prima di qualsiasi elaborazione. La copia viene archiviata nella memoria di backup e consente di ripristinare il file in seguito, ad esempio per eseguire una scansione con database aggiornati.

D

DATABASE

Database creati dagli esperti di Kaspersky Lab contenenti una descrizione dettagliata di tutte le minacce alla sicurezza del computer attualmente esistenti nonché dei metodi per rilevarle ed eliminarle. I database vengono costantemente aggiornati da Kaspersky Lab al presentarsi di nuove minacce. Per ottenere una migliore qualità di rilevamento delle minacce, è consigliabile copiare regolarmente i database dai server degli aggiornamenti di Kaspersky Lab.

DATABASE DELLA POSTA

Database contenenti gli indirizzi email in un formato speciale e salvati sul vostro computer. Ogni ingresso / uscito e-mail è inserito nel database di posta dopo che è stato ricevuto / inviato. I database vengono esaminati durante la scansione completa del computer.

I messaggi in entrata e in uscita vengono analizzati per verificare la presenza di virus in tempo reale al momento dell'invio e della ricezione se la protezione in tempo reale è abilitata.

DATABASE PER IL FILTRAGGIO DEI CONTENUTI

Database creati da tecnici di Kaspersky Lab che contengono esempi di spam e tipica terminologia di spam (parole e frasi). L'applicazione esegue un'analisi linguistica del contenuto delle email de degli allegati basata su su questo database. I database sono regolarmente aggiornati da Kaspersky Lab. Di conseguenza, è necessario che gli amministratori eseguano regolarmente gli aggiornamenti dei database utilizzati dall'applicazione.

DISINFEZIONE DEGLI OGGETTI

Metodo utilizzato per elaborare gli oggetti infetti che consente di recuperare completamente o parzialmente i dati; in caso contrario l'oggetto viene considerato non disinfettabile. La disinfezione degli oggetti viene eseguita in base alle voci dei database. Se la disinfezione è l'azione primaria da eseguire sull'oggetto (ovvero la prima azione da eseguire non appena viene rilevato), dell'oggetto viene creata una copia di backup prima di tentare la disinfezione. Durante la disinfezione è

possibile che parte dei dati venga persa. Questa copia di backup può essere utilizzata per ripristinare lo stato originario dell'oggetto.

DISINFEZIONE DEGLI OGGETTI AL RIAVVIO

Metodo di elaborazione degli oggetti infetti utilizzati da altre applicazioni al momento della disinfezione. Consiste nel creare una copia dell'oggetto infetto, disinfettare la copia creata e sostituire l'oggetto infetto originale con la copia disinfettata dopo il riavvio successivo del sistema.

E

ELIMINAZIONE DEL MESSAGGIO

Metodo di elaborazione di un messaggio di posta contenente tracce di spam che consente di eliminare il messaggio fisicamente. L'applicazione di questo metodo è consigliata per i messaggi contenenti inequivocabilmente spam. Prima di eliminare un messaggio, ne viene salvata una copia nella cartella di backup (a meno che questa opzione non sia disabilitata).

ELIMINAZIONE DI UN OGGETTO

Metodo di elaborazione dell'oggetto che implica la sua eliminazione fisica dalla posizione originaria (disco rigido, cartella, risorsa di rete). Si consiglia di applicare questo metodo agli oggetti pericolosi che, per qualsiasi ragione, non possono essere disinfettati.

ESCLUSIONE

Per esclusione si intende un oggetto escluso dalla scansione da parte dell'applicazione Kaspersky Lab. Prima di eliminare un messaggio, ne viene salvata una copia nella cartella di backup (a meno che questa opzione non sia disabilitata). A ogni attività può essere assegnato un insieme di esclusioni.

F

FALSO ALLARME

Situazione in cui l'applicazione Kaspersky Lab considera un oggetto non infetto come infetto a causa del codice simile a quello di un virus.

FILE CHIAVE

File con l'estensione key, che rappresenta la "chiave" personale che consente di utilizzare l'applicazione Kaspersky Lab. Un file chiave viene incluso nel prodotto acquistato presso i distributori Kaspersky Lab o inviato tramite posta elettronica se l'acquisto avviene online.

FILE COMPRESSO

File di archivio contenente un programma di decompressione e istruzioni di esecuzione per il sistema operativo.

H

HOST

Computer dove è in esecuzione un software server. Un host può eseguire diversi programmi server - per esempio, un server FTP, un mail server, e un Web server possono essere eseguiti dallo stesso host. Gli utenti usano un programma client per accedere all'host (come un browser Web). Anche il termine "server" viene spesso usato per riferirsi al computer che esegue software server, che sfuma la differenza tra un server e un host.

Nelle telecomunicazioni un host è un computer che invia informazioni (come flie via FTP, notizie, o pagine web). Nell'ambito di Internet, gli host sono spesso definiti nodi.

I

INTERCETTORE

Sottocomponente dell'applicazione responsabile della scansione di tipi specifici di messaggi di posta elettronica. Il set di intercettori specifico dell'installazione dipende dal ruolo o dalla combinazione di ruoli per i quali l'applicazione è stata distribuita.

INTERNET PROTOCOL (IP)

Il protocollo di base per Internet, utilizzato senza modifiche dal momento del suo sviluppo nel 1974. Si esegue le operazioni fondamentali come trasmissione dei dati da un computer a un altro e serve come base per protocolli di livello superiore come TCP e UDP. Gestisce la connessione e l'elaborazione degli errori. Il ricorso a tecnologie come il NAT e il mascheramento consente di nascondere un gran numero di reti private attraverso un numero limitato di indirizzi IP (o persino un solo indirizzo). In questo modo diventa possibile gestire le richieste dell'area Internet in costante espansione attraverso uno spazio degli indirizzi IPv4 relativamente limitato.

INTESTAZIONE

Informazioni all'inizio di un file o di un messaggio, composte da dati di basso livello sullo stato e l'elaborazione del file (o del messaggio). In particolare, l'intestazione del messaggio di posta elettronica contiene dati come le informazioni sul mittente e sul destinatario, nonché la data.

L

LICENZA AGGIUNTIVA

Licenza che è stata aggiunta per il funzionamento dell'applicazione Kaspersky Lab ma non è stata attivata. La licenza aggiuntiva viene attivata alla scadenza della licenza attiva.

LICENZA ATTIVA

La licenza attualmente utilizzata per il funzionamento un'applicazione Kaspersky Lab. La licenza definisce la data di scadenza per le funzionalità complete e i criteri di licenza per l'applicazione. Non è possibile disporre di più di una licenza con lo stato attivo.

LIVELLO CONSIGLIATO

Livello di protezione basato sulle impostazioni dell'applicazione consigliate dagli esperti di Kaspersky Lab per fornire il livello di protezione ottimale del computer. Questo livello viene impostato per essere utilizzato per impostazione predefinita.

LIVELLO DI GRAVITÀ DELL'EVENTO

Descrizione dell'evento, registrato durante il funzionamento dell'applicazione Kaspersky Lab. Esistono quattro livelli di gravità:

- **Eventi critici.**
- **Errori funzionali.**
- **Avvisi.**
- **Messaggi informativi.**

Eventi dello stesso tipo possono avere livelli di gravità diversi, in base alla situazione in cui si sono verificati.

M

MASCHERA DI FILE

Per esclusione si intende un oggetto escluso dalla scansione da parte dell'applicazione Kaspersky Lab. I due caratteri jolly standard utilizzati nelle maschere file sono * e ?, dove * rappresenta una qualsiasi combinazione di caratteri e ?

indica un qualsiasi singolo carattere. Utilizzando questi caratteri jolly, è possibile rappresentare qualsiasi file. Notare che il nome e l'estensione sono sempre separati da un punto.

MEMORIA DI BACKUP

Cartella di archiviazione speciale per le copie dei dati di Administration Server creati mediante una utilità di backup.

MESSAGGIO OSCENO

Messaggio email contenente linguaggio offensivo.

MESSAGGIO SOSPETTO

Messaggio che non può essere considerato spam, ma risulta sospetto al momento della scansione (e.g., alcuni tipi di invio mail e di messaggi pubblicitari).

O

OGGETTI DI AVVIO

Cartella nella quale vengono conservati tutti gli oggetti potenzialmente infetti rilevati durante le scansioni o la protezione in tempo reale. Questi oggetti vengono eseguiti ad ogni avvio del sistema operativo. Esistono virus in grado di infettare questi tipi di oggetti in particolare e bloccare, ad esempio, l'accesso al sistema operativo.

OGGETTO OLE

Un oggetto allegato o un oggetto incorporato in un altro file. L'applicazione Kaspersky Lab consente di eseguire la scansione anti-virus degli oggetti OLE. Se ad esempio si inserisce una tabella di Microsoft Office Excel in un documento di Microsoft Office Word, tale tabella verrà esaminata come oggetto OLE.

OGGETTO INFETTO

Oggetto contenente codice dannoso: viene rilevato quando una sezione del codice dell'oggetto corrisponde in modo preciso a una sezione del codice di una minaccia nota. Kaspersky Lab sconsiglia l'uso di oggetti di questo tipo poiché potrebbero causare un'infezione nel computer.

OGGETTO MONITORATO

File trasferito mediante i protocolli HTTP, FTP o SMTP attraverso il firewall e inviato all'applicazione Kaspersky Lab per essere sottoposto a scansione.

OGGETTO PERICOLOSO

Oggetto contenente un virus. Si sconsiglia di accedere a questi oggetti perché ciò potrebbe determinare un'infezione del computer. Una volta rilevato un oggetto infetto, si consiglia di disinfettarlo tramite una delle applicazioni di Kaspersky Lab o di eliminarlo se non è possibile eseguire l'operazione.

OGGETTO POTENZIALMENTE INFETTABILE

Oggetto che, a causa della sua struttura o formato, può essere utilizzato dagli intrusi come "contenitore" per memorizzare e distribuire un oggetto dannoso. Solitamente, si tratta di file eseguibili, ad esempio file con estensione .com, .exe, .dll e così via. Il rischio di attivare codice dannoso in tali file è estremamente alto.

OGGETTO POTENZIALMENTE INFETTO

Oggetto contenente codice modificato di un virus noto, oppure codice che ricorda quello di un virus, ma non ancora noto a Kaspersky Lab. I file potenzialmente infetti vengono rilevati tramite l'analisi euristica.

OGGETTO SEMPLICE

Corpo del messaggio e-mail o semplici allegati, ad esempio, un file eseguibile. Vedere anche oggetti contenitore.

OGGETTO SOSPETTO

Oggetto contenente codice modificato di un virus noto, oppure codice che ricorda quello di un virus, ma non ancora noto a Kaspersky Lab. Gli oggetti sospetti vengono rilevati mediante l'analisi euristica.

P

PACCHETTO DI AGGIORNAMENTO

Pacchetto di file per l'aggiornamento del software. Viene scaricato da Internet e installato nel computer.

PERIODO DI VALIDITÀ DELLA LICENZA

Periodo di tempo durante il quale è possibile utilizzare tutte le funzionalità dell'applicazione Kaspersky Lab. Questo livello viene impostato per essere utilizzato per impostazione predefinita.Livello di gravità dell'evento. Descrizione dell'evento, registrato durante il funzionamento dell'applicazione Kaspersky Lab. Non è possibile aggiornare i database dell'applicazione.

PORTA DI RETE

Parametro TCP e UDP che determina la destinazione dei pacchetti di dati in formato IP trasmessi a un host tramite una rete e che rende possibile l'esecuzione di vari programmi su un host unico per ricevere i dati indipendentemente l'uno dall'altro. Ogni programma processa dati ricevuti attraverso una data porta (questo viene riferito talvolta ad un programma "in ascolto" su quella porta).

Per alcuni protocolli di rete comuni, esistono in genere numeri di porta standard (ad esempio i server Web in genere ricevono richieste HTTP sulla porta TCP 80). I programmi possono tuttavia utilizzare qualsiasi protocollo su qualsiasi porta. Valori possibili: da 1 a 65535.

PROCESSO ATTENDIBILE

Processo dell'applicazione le cui operazioni sui file non vengono monitorate dall'applicazione di Kaspersky Lab in modalità di protezione in tempo reale. In altre parole, nessun oggetto eseguito, aperto o salvato dal processo considerato attendibile verrà esaminato.

PROTEZIONE IN TEMPO REALE

Modalità operativa dell'applicazione che consente di eseguire la scansione degli oggetti per verificare la presenza di codice dannoso in tempo reale.

Ogni programma elabora i dati ricevuti attraverso una determinata porta.Talvolta il programma viene definito "in ascolto" sulla porta. Gli oggetti non infetti vengono restituiti all'utente, quelli contenenti minacce o per i quali si sospetta la presenza di una minaccia vengono elaborati in base alle impostazioni dell'attività e quindi disinfettati, eliminati o messi in Quarantena.

PROTEZIONE MASSIMA

Livello di protezione per il computer corrispondente alla protezione più completa che l'applicazione è in grado di offrire. Con questo livello di protezione, tutti i file presenti sul computer, supporti rimovibili e unità di rete vengono sottoposti a una scansione anti-virus se collegati al computer.

PROTOCOLLO

Set di regole chiaramente definite e standardizzate che regolano l'interazione tra un client e un server. Protocolli noti, e servizi associati ad essi includono HTTP (WWW), FTP, e NNTP (news).

Q

QUARANTENA

Cartella nella quale vengono conservati tutti gli oggetti potenzialmente infetti rilevati durante le scansioni o la protezione in tempo reale.

R

RIPRISTINO

Spostamento di un oggetto originale dalla sezione Quarantena o Backup alla cartella in cui era stato inizialmente trovato prima di essere disinfettato, eliminato, spostato nella Quarantena o in una cartella diversa specificata dall'utente.

S

SOCKS

Protocollo del server proxy che consente di stabilire una connessione punto-punto tra computer nelle reti interne ed esterne.

SALTARE GLI OGGETTI

Metodo di elaborazione in base al quale un oggetto viene passato all'utente senza alcuna modifica. Se la registrazione degli eventi è abilitata per questo tipo di evento, le informazioni sull'oggetto rilevato verranno registrate nel rapporto.

SCANSIONE ARCHIVIAZIONE

Scansione dei messaggi e-mail archiviati sul server di posta e il contenuto delle cartelle condivise utilizzando la versione più recente del database. La scansione viene eseguita in background e può essere eseguita utilizzando una pianificazione o su richiesta dell'utente. Vengono esaminate tutte le cartelle condivise e l'archivio delle caselle di posta. Durante la scansione è possibile che vengano rilevati virus per i quali non erano disponibili informazioni nel database durante le scansioni precedenti.

SCANSIONE DEL TRAFFICO

Scansione in tempo reale che utilizza informazioni dell'ultima versione dei database per gli oggetti trasmessi attraverso tutti i protocolli, ad esempio HTTP, FTP e così via.

SCANSIONE DEL TRAFFICO

La subnet mask (nota anche come netmask) e l'indirizzo di rete determinano gli indirizzi dei computer in una rete.

SCANSIONE MANUALE

Modalità operativa dell'applicazione di Kaspersky Lab avviata dall'utente in grado di gestire qualsiasi file presente sul computer.

SCRIPT

Un piccolo programma per computer o una porzione indipendente di un programma (funzione) normalmente sviluppato per eseguire una piccola attività specifica. Viene utilizzato molto spesso con programmi incorporati in ipertesto. Gli script vengono eseguiti, ad esempio, all'apertura di determinati siti Web.

Se è abilitata la protezione in tempo reale, l'applicazione controllerà gli script all'avvio, intercettandoli ed esaminandoli per verificare la presenza di virus. In funzione dei risultati della scansione, è possibile bloccarne o consentirne l'esecuzione.

SERVER DEGLI AGGIORNAMENTI DI KASPERSKY LAB

Elenco dei server HTTP e FTP di Kaspersky Lab da cui l'applicazione scarica database e aggiornamenti dei moduli nel computer.

SETTORE DI AVVIO DEL DISCO

Un settore di avvio è una determinata area sul disco rigido, su floppy o su altri dispositivi di memorizzazione dei dati del computer. Contiene informazioni sul file system del disco e un programma di caricamento responsabile dell'avvio del sistema operativo.

In particolare può anche memorizzare ed elaborare richieste inverse, determinando il nome di un host in base al relativo indirizzo IP (record PTR). L'applicazione Kaspersky Lab consente di esaminare i settori di avvio per verificare la presenza di virus e di disinfettarli se viene rilevata un'infezione.

SOGLIA DI ATTIVITÀ VIRUS

Livello massimo consentito per un tipo specifico di evento in un periodo di tempo limitato che, se superato, verrà considerato come attività eccessiva del virus e minaccia di un attacco di virus. Questa funzionalità è molto importante durante gli attacchi di virus e consente a un amministratore di reagire con tempestività alle minacce di attacchi che si presentano.

SPAM

Invio di massa di messaggi di posta elettronica non richiesti, spesso contenenti messaggi pubblicitari.

SPOSTAMENTO DI OGGETTI IN QUARANTENA

Metodo di elaborazione di un oggetto potenzialmente infetto attraverso il blocco dell'accesso al file e lo spostamento dalla posizione originale alla cartella Quarantena, in cui viene salvato in forma crittografata, in modo da eliminare la minaccia di infezione. Gli oggetti in quarantena possono essere esaminati utilizzando i database Anti-Virus aggiornati, analizzati dall'amministratore o inviati a Kaspersky Lab.

STATO DELLA PROTEZIONE

Stato corrente della protezione che indica il livello di sicurezza del computer.

T

TECNOLOGIA ICHECKER

iChecker è una tecnologia che consente di accelerare la scansione anti-virus escludendo gli oggetti che sono rimasti inalterati dall'ultima scansione, sempre che i parametri di scansione, ovvero le impostazioni e il database anti-virus, non siano stati modificati. Le informazioni di ogni file vengono memorizzate in un database speciale. Questa tecnologia viene utilizzata nelle modalità di protezione in tempo reale e di scansione manuale.

Si supponga, ad esempio, che a un archivio esaminato da Kaspersky Lab sia stato assegnato lo stato non infetto. Alla scansione successiva, l'applicazione ignorerà questo archivio, a meno che non sia stato modificato o non siano state modificate le impostazioni di scansione. Se il contenuto dell'archivio è stato modificato aggiungendo un nuovo oggetto, oppure sono state modificate le impostazioni di scansione o è stato aggiornato il database anti-virus, l'archivio verrà esaminato nuovamente.

Limitazioni della tecnologia iChecker:

- questa tecnologia non rappresenta la scelta ideale con i file di grandi dimensioni in quanto risulta più veloce esaminare un file che controllare se sia stato modificato dall'ultima scansione;
- la tecnologia supporta un numero limitato di formati (.exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

V

VIRUS DI BOOT

Virus che infetta i settori di avvio dell'unità disco rigido di un computer. Il caricamento del virus all'interno del sistema viene forzato durante il riavvio dal virus stesso e il codice del virus assume il controllo diretto al posto del codice del programma di avvio originale.

VIRUS SCONOSCIUTO

Nuovo virus su cui non sono disponibili informazioni nei database. In genere i virus sconosciuti vengono rilevati dall'applicazione negli oggetti mediante l'analisi euristica e tali oggetti vengono classificati come potenzialmente infetti.

W

WHITE LIST DI INDIRIZZI

Elenco di indirizzi di posta elettronica che inviano i messaggi che non è necessario sottoporre a scansione da parte dell'applicazione Kaspersky Lab.

KASPERSKY LAB

Fondata nel 1997. Kaspersky Lab rappresenta oggi una delle aziende leader nello sviluppo di una vasta gamma di prodotti software ad elevate prestazioni destinati alla protezione delle informazioni, tra cui sistemi anti-virus, anti-spam e anti-hacking.

Kaspersky Lab è una società internazionale. La sede centrale si trova nella Federazione russa e gli uffici di rappresentanza sono nel Regno Unito, in Francia, Germania, Giappone, nei paesi del Benelux, in Cina, Polonia, Romania e negli USA (California). Recentemente è stata inaugurata una nuova sede, l'European Anti-Virus Research Centre, in Francia. La rete di partner di Kaspersky Lab è costituita da oltre 500 aziende in tutto il mondo.

Degli oltre 1000 specialisti qualificati che lavorano presso Kaspersky Lab, 10 hanno conseguito un Master di specializzazione post laurea in Business Administration e 16 un dottorato di ricerca. Tutti gli esperti anti-virus Kaspersky Lab senior sono membri dell'organizzazione CARO (Computer Anti-Virus Researchers Organization).

I punti di forza dell'azienda sono la notevole competenza e la significativa esperienza maturata in quattordici di anni di intensa attività di sviluppo di efficaci soluzioni anti-virus. Un'analisi approfondita delle attività dei virus informatici consente agli specialisti dell'azienda di anticipare le tendenze nello sviluppo di malware e di offrire agli utenti una protezione efficace e tempestiva contro nuovi tipi di attacchi. Questo vantaggio sta alla base dei prodotti e dei servizi offerti da Kaspersky Lab. I prodotti dell'azienda sono sempre un passo avanti rispetto a quelli della concorrenza nell'ambito della protezione anti-virus.

L'esperienza maturata in anni di duro lavoro hanno rafforzato nel tempo la posizione dominante raggiunta oggi. Kaspersky Lab è stata la prima azienda a sviluppare molti degli standard per software anti-virus moderni. Il prodotto di punta, Kaspersky Anti-Virus®, protegge in modo efficace tutti i tipi di sistemi dagli attacchi dei virus, incluse le workstation, i file server, i sistemi di posta, i firewall, i gateway Internet e i computer palmari. Gli strumenti di facile gestione di cui è fornito consentono di automatizzare la protezione anti-virus di computer e reti aziendali. Un gran numero di sviluppatori di fama internazionale utilizza il kernel di Kaspersky Anti-Virus nei propri prodotti, inclusi Nokia ICG (USA), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India) e BorderWare (Canada).

I clienti di Kaspersky Lab possono usufruire di una vasta gamma di servizi aggiuntivi che garantiscono il funzionamento costante dei prodotti e una compatibilità completa con i propri requisiti specifici. L'azienda progetta, implementa e supporta sistemi anti-virus aziendali. Il database anti-virus di Kaspersky Lab viene aggiornato ogni ora. Il servizio di supporto tecnico offerto ai clienti è disponibile 24 ore su 24, in diverse lingue.

Per porre domande, fare commenti o ricevere consigli, è possibile contattarci tramite i rivenditori o direttamente presso Kaspersky Lab. Tutta l'assistenza necessaria in relazione alle questioni sollevate sui prodotti Kaspersky verrà fornita tramite telefono o posta elettronica. Viene sempre garantita una risposta completa e dettagliata a qualsiasi domanda.

Sito ufficiale di Kaspersky Lab:	http://www.kaspersky.it
Enciclopedia dei Virus:	http://www.viruslist.com
Anti-Virus Lab:	newvirus@kaspersky.com (solo per l'invio di archivi di oggetti sospetti) http://support.kaspersky.ru/virlab/helpdesk.html?LANG=it (per domande agli analisti anti-virus)

CONTRATTO DI LICENZA

AVVERTENZA LEGALE IMPORTANTE PER TUTTI GLI UTENTI: LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO PRIMA DI INIZIARE A USARE IL SOFTWARE.

FACENDO CLIC SUL PULSANTE ACCETTO NELLA FINESTRA DEL CONTRATTO DI LICENZA O IMMETTENDO IL/I SIMBOLO/I CORRISPONDENTE/I, LEI ACCETTA DI ESSERE VINCOLATO AL RISPETTO DEI TERMINI E DELLE CONDIZIONI DI QUESTO CONTRATTO. **TALE AZIONE EQUIVALE AD APPORRE LA SUA FIRMA E SIGNIFICA CHE ACCETTA DI ESSERE VINCOLATO E DI DIVENTARE UNA PARTE CONTRAENTE DEL PRESENTE CONTRATTO E CHE ACCETTA LA VALIDITÀ LEGALE DEL PRESENTE CONTRATTO COME QUALSIASI ACCORDO STIPULATO PER ISCRITTO E DA LEI FIRMATO**. SE NON È D'ACCORDO CON TUTTI I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO, ANNULLI L'INSTALLAZIONE DEL SOFTWARE E NON LO INSTALLI.

DOPO AVER CLICCATO IL PULSANTE "ACCETTO" NELLA FINESTRA DEL CONTRATTO DI LICENZA O DOPO AVER IMMESSO IL/I SIMBOLO/I CORRISPONDENTE/I LEI HA IL DIRITTO DI USARE IL SOFTWARE SECONDO I TERMINI E LE CONDIZIONI DEL PRESENTE CONTRATTO.

1. **Definizioni**

1.1 **Per Software** si intende il software, compresi gli aggiornamenti e i relativi materiali.

1.2. **Per Titolare** (titolare di tutti i diritti, sia esclusivi che non, relativi al Software) si intende Kaspersky Lab ZAO, una società regolarmente costituita ai sensi delle leggi della Federazione Russa.

1.3. **Per Computer** si intende l'hardware, ivi compresi i personal computer, i laptop, le postazioni di lavoro, i personal digital assistant, gli "smart phone", i dispositivi palmari o gli altri dispositivi elettronici per cui il Software è stato progettato su cui il Software verrà installato e/o utilizzato.

1.4. **Per Utente Finale (Lei/Suo)** si intende il soggetto o i soggetti che installano o utilizzano il Software per proprio conto e che sta/stanno utilizzando legalmente una copia del Software; o, se il Software è stato scaricato o installato per conto di un'organizzazione, ad esempio da un dipendente, *"Lei"* sta a intendere anche l'organizzazione per cui il Software è stato scaricato o installato e si dichiara con il presente che tale organizzazione ha autorizzato quel soggetto ad accettare questo contratto, scaricando e installando il Software per conto dell'organizzazione stessa. Ai fini del presente contratto il termine *"organizzazione"* include, a titolo esemplificativo e non limitativo, qualsiasi società di persone, società a responsabilità limitata, persona giuridica, associazione, società per azioni, trust, joint venture, organizzazione sindacale, organizzazione non registrata o autorità governativa.

1.5. **Per Partner** si intendono le organizzazioni o il soggetto/i soggetti che distribuiscono il Software al Titolare sulla base di un contratto e di una licenza.

1.6. **Per Aggiornamento/i** si intendono tutti gli aggiornamenti, le revisioni, le patch, i perfezionamenti, le correzioni, le modifiche, le copie, le aggiunte o i pacchetti di manutenzione, ecc.

1.7. **Per Manuale dell'Utente** si intende il manuale dell'utente, la guida per l'amministratore, il libro di riferimento e i relativi materiali di tipo illustrativo o di altro tipo.

2. **Concessione della licenza**

2.1. Con il presente il Titolare Le concede licenza di uso non esclusivo per la memorizzazione, il caricamento, l'installazione, l'esecuzione e la visualizzazione (l'"uso") del Software su di una quantità specificata di Computer al fine di fornire un supporto per la protezione del Suo Computer, sul quale è installato il Software, contro le minacce descritte nel Manuale dell'Utente, in osservanza di tutti i requisiti tecnici descritti nel Manuale dell'Utente e secondo i termini e le condizioni di questo Contratto (la "Licenza") e Lei accetta questa Licenza:

Versione di prova. Se ha ricevuto, scaricato e/o installato la versione di prova del Software e se ha aderito alla licenza di valutazione del Software, può utilizzare il Software solo a scopo dimostrativo e soltanto per il periodo dimostrativo consentito, salvo laddove diversamente indicato, a partire dalla data della prima installazione. È severamente proibito l'uso del Software per scopi diversi o per un periodo più lungo del periodo di valutazione consentito.

Software per ambiente multiplo; Software a linguaggio multiplo; Software a doppio supporto magnetico; Copie multiple; Servizi aggiuntivi. Qualora Lei utilizzi diverse versioni del Software o edizioni del Software di lingua diversa, o riceva il Software su diversi supporti magnetici, o comunque riceva copie multiple del Software, ovvero qualora in cui Lei abbia acquistato il Software insieme a software aggiuntivi, il numero massimo di Computer su cui il Software può essere installato equivale al numero di licenze ricevuto dal Titolare *sempre che* ogni licenza acquistata Le dia diritto a installare e utilizzare il Software sulla quantità numero di Computer specificata nei paragrafi 2.2 e 2.3, salvo laddove diversamente stabilito dai termini della licenza.

2.2. Se il Software è stato acquistato su un supporto fisico, Lei ha il diritto di utilizzare il Software per proteggere la quantità di Computer specificata nel pacchetto Software.

2.3. Se il Software è stato acquistato via Internet, Lei ha il diritto di utilizzare il Software per la protezione della quantità di Computer specificata all'atto dell'acquisto della Licenza del Software.

2.4. Lei ha diritto di copiare il Software soltanto a scopo di back-up e solo a titolo di sostituzione della copia di Sua legale proprietà, qualora essa vada persa, distrutta o diventi inutilizzabile. Questa copia di back-up non può essere utilizzata per fini diversi e deve essere distrutta quando viene meno il diritto d'uso del Software o alla scadenza della Sua licenza o qualora questa venga meno per qualsiasi altro motivo, ai sensi dalla legislazione in vigore nel principale paese di residenza o nel paese in cui Lei fa uso del Software.

2.5. Lei ha la facoltà di trasferire il diritto non esclusivo di licenza d'uso del Software ad altri soggetti o persone giuridiche previste dalla licenza concessaLe dal Titolare, purché il beneficiario accetti di essere vincolato da tutti i termini e dalle condizioni del presente Contratto e La sostituisca in toto nel godimento della licenza concessa dal Titolare. In caso di trasferimento di tutti i diritti d'uso del Software concessi dal Titolare, Lei è tenuto a distruggere tutte le copie del Software, ivi compresa la copia di back-up. Se Lei è il beneficiario della licenza così trasferita, deve accettare di osservare tutti i termini e le condizioni del presente Contratto. Se Lei non accetta di essere vincolato da tutti i termini e le condizioni del presente Contratto, non Le è permesso installare e/o fare uso del Software. In qualità di beneficiario della licenza trasferita, Lei riconosce inoltre di non detenere altri diritti o diritti migliori rispetto a quelli che spettavano all'Utente Finale che ha acquistato il Software dal Titolare.

2.6. Dal momento in cui si procede all'attivazione del Software o dopo l'installazione del file della chiave di licenza (a eccezione della versione di prova del Software), Lei ha diritto di ricevere i seguenti servizi per il periodo di tempo specificato sul pacchetto Software (se il Software è stato acquistato su supporto fisico) o specificato durante l'acquisto (se il Software è stato acquistato via Internet):

- Aggiornamenti del Software via Internet quando e nel momento in cui il Titolare li pubblica sul suo sito o attraverso altri servizi online. Qualsiasi Aggiornamento di cui Lei possa essere destinatario costituisce parte del Software e a esso si applicano i termini e le condizioni di questo Contratto;

- Supporto Tecnico via Internet e Hotline telefonica di Supporto Tecnico.

3. **Attivazione e validità**

3.1. Nel caso in cui Lei apportasse modifiche al Suo computer o al software di altri fornitori installato su di esso, il Titolare ha la facoltà di chiederLe di ripetere l'attivazione del Software o l'installazione del file della chiave di licenza. Il Titolare si riserva il diritto di utilizzare qualsiasi mezzo e qualsiasi procedura per verificare la validità della Licenza e/o la validità legale della copia del Software installata e/o utilizzata sul Suo Computer.

3.2. Se il Software è stato acquistato su supporto fisico, esso può essere utilizzato previa accettazione del presente Contratto per il periodo specificato sulla confezione a far data dalla data di accettazione del presente Contratto.

3.3. Se il Software è stato acquistato via Internet, il Software può essere utilizzato previa accettazione del presente Contratto per il periodo specificato durante l'acquisto.

3.4. Lei ha diritto di usare la versione di prova del Software secondo quanto disposto dal Paragrafo 2.1 senza alcun addebito unicamente per il periodo di valutazione (30 giorni) concesso dal momento della sua attivazione ai sensi del presente Contratto, *purché* la versione di prova non dia diritto ad Aggiornamenti e a Supporto Tecnico via Internet e tramite Hotline telefonica.

3.5. La Sua Licenza d'Uso del Software è limitata al periodo di tempo specificato nei Paragrafi 3.2 o 3.3 (secondo quanto applicabile) e nel periodo restante può essere visionata utilizzando i supporti descritti nel Manuale dell'Utente.

3.6. Nel caso in cui Lei abbia acquistato il Software per un utilizzo su più di un Computer, la Sua Licenza d'Uso del Software è limitata al periodo di tempo che ha inizio alla data di attivazione del Software o l'installazione del file della chiave di licenza sul primo Computer.

3.7. Fatto salvo qualsiasi altro rimedio previsto dalla legge o basato sui principi di opportunità, giustizia e onesta composizione ("equity") a cui il Titolare possa legittimamente fare ricorso, nel caso di una Sua violazione dei termini e delle condizioni del presente Contratto, il Titolare avrà diritto in ogni momento e senza obbligo di preavviso di rescindere questa Licenza d'uso del Software senza rimborsare il prezzo d'acquisto né parte di esso.

3.8. Lei accetta di fare uso del Software e utilizzare qualsiasi rapporto o informazione derivante dall'utilizzo di questo Software in modo conforme a tutte le leggi applicabili internazionali, nazionali, statali, regionali e locali e a qualsiasi normativa, ivi compresa, a titolo esemplificativo e non limitativo, le leggi sulla privacy, sui diritti d'autore, sul controllo delle esportazioni e sulle oscenità.

3.9. Fatte salve eventuali disposizioni contrarie specificamente previste in questa sede, Lei non ha la facoltà di trasferire né di assegnare alcuno dei diritti che le sono stati concessi ai sensi del presente Contratto né alcuno degli obblighi che da esso Le derivano.

4. **Supporto Tecnico**

Il Supporto Tecnico descritto al Paragrafo 2.6 del presente Contratto Le viene fornito quando è stato installato l'Aggiornamento più recente del Software (a eccezione della versione di prova del Software).

Servizio di assistenza tecnica: http://support.kaspersky.com

5. **Restrizioni**

5.1. Le è fatto divieto di emulare, clonare, locare, dare in prestito, noleggiare, vendere, modificare, decompilare o reingegnerizzare il Software, disassemblarlo o creare opere accessorie basate sul Software o su una porzione di esso con la sola eccezione di diritti non rinunciabili previsti dalla legislazione applicabile, e Le è fatto comunque divieto di ridurre parte del Software in forma decifrabile o trasferire il Software tutelato da licenza o qualsivoglia sottoinsieme dello stesso, o permettere a terzi di fare quanto sopra, salvo nella misura in cui le limitazioni sopra illustrate siano espressamente proibite dal diritto applicabile. È fatto divieto di utilizzare o reingegnerizzare qualsivoglia codice binario o origine del Software allo scopo di ricreare l'algoritmo del programma, che è proprietario. Tutti i diritti non espressamente concessi attraverso il presente Contratto sono riservati al Titolare e/o ai suoi fornitori, secondo quanto applicabile. L'uso non autorizzato del Software produrrà la rescissione immediata e automatica del presente Contratto e della Licenza concessa in virtù dello stesso e può determinare l'apertura di un procedimento legale nei Suoi confronti.

5.2. Fatto salvo quanto disposto al Paragrafo 2.5 del presente Contratto, Lei non ha diritto di trasferire i diritti d'uso del Software a terzi.

5.3. Le è fatto divieto di mettere a conoscenza di terzi il codice di attivazione e/o il file chiave della licenza o di consentire l'accesso al codice di attivazione e/o di licenza, i quali rappresentano dati riservati del Titolare; Lei sarà inoltre tenuto a usare ogni ragionevole cautela per la protezione del codice di attivazione e/o di licenza riservati, qualora Lei abbia la facoltà di trasferire il codice di attivazione e/o di licenza a terzi secondo quanto illustrato al Paragrafo 2.5 del presente Contratto.

5.4. Non è consentito concedere a noleggio, in locazione o in prestito a terzi il Software.

5.5. Non è consentito utilizzare il Software per la creazione di dati o di software che servono a individuare, bloccare o gestire le minacce descritte nel Manuale dell'Utente.

5.6. In caso di violazione dei termini e delle condizioni del presente Contratto, il Titolare ha il diritto di bloccare il file di codice o di annullare la Sua licenza d'uso del Software senza obbligo di rimborso.

5.7. Se si usa la versione di prova del Software non si ha il diritto di ricevere il Supporto Tecnico specificato al Paragrafo 4 del presente Contratto, né il diritto di trasferire la licenza o i diritti d'uso del software a terzi.

6. **Garanzia limitata e clausola di esclusione della responsabilità**

6.1. Il Titolare garantisce che il Software eseguirà sostanzialmente le prestazioni illustrate nelle specifiche e descritte nel Manuale dell'Utente *fermo restando, tuttavia, che* tale garanzia limitata non si applica a quanto segue: (w) lacune del Suo Computer e relative violazioni per le quali il Titolare declina espressamente qualsiasi

responsabilità di garanzia; (x) malfunzionamenti, difetti o guasti conseguenti a cattivo uso, abuso, incidente, negligenza, difetti di installazione, funzionamento o manutenzione, furto, atto vandalico, evento di forza maggiore, atti di terrorismo, interruzione di tensione o momentanea sovratensione, infortunio, alterazione, modifica non consentita o riparazioni eseguite da soggetti diversi dal Titolare o qualsiasi azione o causa, a opera Sua o di qualsiasi altro soggetto terzo, ragionevolmente fuori del controllo del Titolare; (y) qualsiasi difetto da Lei tenuto nascosto al Titolare anche dopo la comparsa della prima anomalia; e (z) incompatibilità provocata da componenti hardware e/o software installati sul Suo computer.

6.2. Lei riconosce, accetta e concorda che nessun software è esente da errori e che Lei è stato informato che è necessario fare il back-up del Computer, con la frequenza e secondo le modalità per Lei più indicate.

6.3. In caso di violazione dei termini descritti nel Manuale dell'Utente o nel presente Contratto, il Titolare non garantisce il corretto funzionamento del Software.

6.4. Il Titolare non garantisce che il Software funzionerà correttamente se Lei non scarica regolarmente gli Aggiornamenti specificati nel Paragrafo 2.6 del presente Contratto.

6.5. Il Titolare non garantisce la protezione dalle minacce descritte nel Manuale dell'Utente una volta scaduto il periodo specificato nei Paragrafi 3.2 or 3.3 del presente Contratto o una volta scaduta, per qualsiasi motivo, la Licenza d'uso del Software.

6.6. IL SOFTWARE VIENE FORNITO "COSÌ COM'È" E IL TITOLARE NON FA ALCUNA DICHIARAZIONE E NON FORNISCE ALCUNA GARANZIA IN QUANTO A USO O PRESTAZIONI. FATTE SALVE LE GARANZIE, LE CONDIZIONI, LE DICHIARAZIONI O I TERMINI CHE NON POSSONO ESSERE ESCLUSI O LIMITATI DAL DIRITTO APPLICABILE, IL TITOLARE E I SUOI PARTNER, NON FORNISCONO ALCUNA GARANZIA, CONDIZIONE, DICHIARAZIONE O TERMINE (NÉ ESPLICITO NÉ IMPLICITI NÉ PREVISTO DALLA LEGGE, DALLA COMMON LAW, DALLE CONSUETUDINI O DAGLI USI O ALTRO) IN MERITO A QUALSIVOGLIA QUESTIONE, IVI COMPRESE, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, LA NON VIOLAZIONE DEI DIRITTI DI TERZI, LA COMMERCIABILITÀ, LA QUALITÀ SODDISFACENTE, L'INTEGRAZIONE O L'APPLICABILITÀ PER UN FINE SPECIFICO. LEI SI ASSUME LA RESPONSABILITÀ DI TUTTI GLI ERRORI E TUTTI I RISCHI RELATIVI ALLE PRESTAZIONI NONCHÉ LA RESPONSABILITÀ DI AVER SCELTO IL SOFTWARE ALLO SCOPO DI RAGGIUNGERE I RISULTATI DESIDERATI NONCHÉ DELL'INSTALLAZIONE DEL SOFTWARE, DEL RELATIVO USO E DEI RISULTATI OTTENUTI DALLO STESSO. SENZA LIMITARE LE DISPOSIZIONI DI CUI SOPRA, IL TITOLARE NON FORNISCE ALCUNA DICHIARAZIONE E NON FORNISCE ALCUNA GARANZIA CHE IL SOFTWARE SARÀ ESENTE DA ERRORI O ESENTE DA INTERRUZIONI O ALTRI DIFETTI DI FUNZIONAMENTO NÉ CHE IL SOFTWARE SARÀ IN GRADO DI SODDISFARE IN TOTO O IN PARTE LE SUE ESIGENZE, SIANO ESSE STATE COMUNICATE AL TITOLARE O MENO.

7. **Esclusione e limite della responsabilità**

NELLA MASSIMA MISURA CONSENTITA DAL DIRITTO APPLICABILE, IN NESSUN CASO IL TITOLARE O I SUOI PARTNER SARANNO RESPONSABILI DI DANNI SPECIALI, MARGINALI, PUNITIVI, INDIRETTI O DI DANNI INDIRETTI DI QUALSIASI TIPO (IVI COMPRESI, A TITOLO ESEMPLIFICATIVO E NON LIMITATIVO, I DANNI PER PERDITA DI UTILI O PER PERDITA DI INFORMAZIONI RISERVATE O DI ALTRE INFORMAZIONI, PER INTERRUZIONE DELL'ATTIVITÀ LAVORATIVA, PER PERDITA DI PRIVACY, PER CORRUZIONE, DANNO E PERDITA DI DATI O DI PROGRAMMI, PER MANCATA OSSERVANZA DI UN OBBLIGO IVI COMPRESO QUALSIASI ONERE IMPOSTO PER LEGGE, DOVERE DI BUONA FEDE O DOVERE DI RAGIONEVOLE DILIGENZA, PER NEGLIGENZA, PER PERDITA ECONOMICA E PER QUALSIASI ALTRA PERDITA PECUNIARIA O ALTRA PERDITA DI SORTA) DERIVANTE DA O IN QUALSIASI MODO COLLEGATO ALL'USO O ALL'IMPOSSIBILITÀ DI USARE IL SOFTWARE, ALLA FORNITURA O MANCATA FORNITURA DEL SERVIZIO DI SUPPORTO O DI ALTRI SERVIZI, INFORMAZIONI, SOFTWARE E RELATIVI CONTENUTI ATTRAVERSO IL SOFTWARE O COMUNQUE DERIVANTI DALL'USO DEL SOFTWARE O COMUNQUE AI SENSI O IN RELAZIONE A QUALSIASI DISPOSIZIONE DEL PRESENTE CONTRATTO, O DERIVANTI DA UNA VIOLAZIONE DEL PRESENTE CONTRATTO O DA QUALSIVOGLIA ILLECITO (IVI COMPRESA LA NEGLIGENZA, LA FALSA TESTIMONIANZA, QUALSIASI OBBLIGO O DOVERE RELATIVI ALLA RESPONSABILITÀ) O DA UNA VIOLAZIONE DI UN OBBLIGO DI LEGGE O DA UNA VIOLAZIONE DELLA GARANZIA DA PARTE DEL TITOLARE O DI UNO DEI SUOI PARTNER, ANCHE QUALORA IL TITOLARE O UNO DEI SUOI PARTNER SIA STATO INFORMATO DELLA POSSIBILITÀ DI TALI DANNI.

LEI ACCETTA CHE NEL CASO IN CUI IL TITOLARE E/O SUOI PARTNER VENISSERO TROVATI RESPONSABILI, LA RESPONSABILITÀ DEL TITOLARE E/O DEI SUOI PARTNER SI LIMITERÀ AL COSTO DEL SOFTWARE. IN NESSUN CASO LA RESPONSABILITÀ DEL TITOLARE E/O DEI SUOI PARTNER POTRÀ SUPERARE LE SOMME VERSATE PER IL SOFTWARE AL TITOLARE O AL PARTNER (SECONDO QUANTO APPLICABILE).

NULLA IN QUESTO CONTRATTO ESCLUDE O LIMITA LA QUALSIVOGLIA RICHIESTA DI DANNI IN CASO DI MORTE E LESIONI PERSONALI. INOLTRE IN CASO IN CUI UNA MANLEVA, ESCLUSIONE O LIMITAZIONE CONTEMPLATE DAL PRESENTE CONTRATTO NON POSSA ESSERE ESCLUSA O LIMITATA AI SENSI DEL DIRITTO APPLICABILE, QUELLA MANLEVA, ESCLUSIONE O LIMITAZIONE NON SARÀ VALIDA NEI SUOI CONFRONTI E LEI DOVRÀ CONTINUARE A OSSERVARE TUTTE LE RESTANTI MANLEVE, ESCLUSIONI E LIMITAZIONI.

8. **GNU e altre licenze di Terzi**

Il Software può comprendere alcuni programmi software sottoposti a licenza (o a sublicenza) dell'utente ai sensi della GNU Licenza Pubblica Generica (General Public License, GPL) o ad altra licenza software di analoga natura che, tra gli altri, concede all'utente il diritto di copiare, modificare e ridistribuire certi programmi o porzioni di essi e di avere accesso al codice source ("Software Open Source"). Se tali licenze prevedono che per un software distribuito in formato binario eseguibile anche il codice source venga reso disponibile ai suoi utenti, il codice source deve essere reso accessibile inviando la richiesta all'indirizzo source@kaspersky.com altrimenti il codice source verrà fornito insieme al Software. Se le licenze dei Software Open Source prevedono che il Titolare fornisca diritti d'uso, di copia e modifica del programma Software Open Source più ampi dei diritti concessi in virtù del presente Contratto, tali diritti avranno la priorità sui diritti e sulle restrizioni contemplati da questo documento.

9. **Proprietà Intellettuale**

9.1 Lei accetta che il Software e il fatto di esserne autori, i sistemi, le idee e i metodi operativi, la documentazione e altre informazioni contenute nel Software, sono proprietà intellettuale esclusiva e/o preziosi segreti commerciali del Titolare o dei suoi partner e che il Titolare e i suoi partner, secondo quanto applicabile, sono protetti dal diritto civile e penale e dalla legge sul copyright, sul segreto commerciale, sul marchio di fabbrica e sui brevetti della Federazione Russa, dell'Unione Europea e degli Stati Uniti e da altri trattati internazionali o di altri paesi. Il presente Contratto non Le concede alcun diritto di proprietà intellettuale né alcun diritto sui marchi o sui marchi di servizio del Titolare e/o dei suoi partner ("Marchi di fabbrica"). Lei ha la facoltà di usare i marchi di fabbrica solo nella misura in cui essi permettono di identificare le stampe prodotte dal Software in conformità con la pratica sui marchi generalmente accettata, ivi compresa l'identificazione del nome del proprietario del Marchio di fabbrica. Tale uso di un Marchio di fabbrica non Le conferisce alcun diritto di proprietà sul Marchio stesso. Il Titolare e/o i relativi partner possiedono e conservano ogni diritto, titolo e interesse relativo e collegato al Software, ivi comprese, senza alcuna limitazione, le correzioni d'errore, i perfezionamenti, gli Aggiornamenti o altre modifiche del Software, sia apportate dal Titolare che da Terzi nonché tutti i diritti d'autore, i brevetti, i diritti su segreti commerciali, i marchi di fabbrica e qualsiasi altro diritto di proprietà intellettuale ivi contemplato. Il possesso, l'installazione o l'uso del Software da parte Sua non Le trasferisce alcun titolo nella proprietà intellettuale del Software e Lei non acquisirà alcun diritto sul Software, salvo nella misura espressamente indicata nel presente Contratto. Tutte le copie del Software eseguite ai sensi del presente documento devono contenere le stesse avvertenze proprietarie che compaiono sul e nel Software. Fatto salvo quanto disposto in questo documento, il presente Contratto non Le conferisce alcun diritto di proprietà intellettuale sul Software e Lei riconosce che la Licenza, secondo la definizione data in seguito, concessa ai sensi del presente Contratto Le conferisce soltanto il diritto di uso limitato ai termini e alle condizioni del presente Contratto. Il Titolare si riserva tutti i diritti che non Le sono espressamente concessi ai sensi del presente Contratto.

9.2 Lei riconosce che il codice source, il codice di attivazione e/o il file di codice di licenza per il Software sono proprietari del Titolare e che essi costituiscono segreto commerciale del Titolare. Lei accetta di non modificare, adattare, reingegnerizzare, decompilare, disassemblare, né comunque tentare di scoprire il codice source del Software.

9.3 Lei accetta di non modificare, né alterare in alcun modo il Software. Lei non ha la facoltà di rimuovere, né di alterare alcuna delle avvertenze in materia di diritti d'autore o altre avvertenze proprietarie sulle copie del Software.

10. **Diritto applicabile; Arbitrato**

Il presente Contratto sarà regolamentato dalle leggi della Federazione Russa e interpretato conformemente a esse, senza riferimento a conflitti fra stato di diritto e principi. Il presente Contratto non sarà regolamentato dalla Convenzione delle Nazioni Unite sui Contratti per la Vendita Internazionale di Merci, la cui applicazione è espressamente esclusa. Qualsiasi vertenza derivante dall'interpretazione o dall'applicazione dei termini del presente Contratto o dalla sua violazione dovrà essere regolata tramite trattativa diretta oppure dal Tribunale dell'Arbitrato Commerciale Internazionale avente sede presso la Camera di Commercio e dell'Industria della Federazione Russa di Mosca, Federazione Russa. Qualsiasi lodo arbitrale emesso dall'arbitro sarà definitivo e vincolante per le parti e qualsiasi giudizio su tale lodo può essere fatto valere in ogni foro competente. Nulla nel presente Paragrafo 10 può impedire a una delle Parti di ricercare e ottenere equo indennizzo presso un foro competente, sia prima, durante sia dopo il processo d'arbitrato.

11. **Periodo di validità per la presentazione di azioni legali**

    A prescindere dalla forma, nessuna azione derivante dalle transazioni commerciali eseguite ai sensi del presente Contratto può essere presentata dalle due parti contrattuali a più di un (1) anno dal momento in cui è accaduto o si è scoperto che è accaduto l'evento su cui si basa l'azione, tranne in caso di azioni per violazione dei diritti di proprietà intellettuale, che possono essere presentate entro il periodo massimo applicabile secondo i termini di legge.

12. **Totalità del Contratto; Clausola salvatoria; Assenza di deroga**

    Il presente Contratto costituisce l'intero contratto tra Lei e il Titolare e sostituisce ogni altro accordo, proposta, comunicato o comunicato commerciale precedente, sia verbale che scritto, relativo al Software o relativo al presente Contratto. Lei riconosce di aver letto il presente Contratto, lo comprende e accetta di essere vincolato ai suoi termini e condizioni. Se un foro competente giudica una qualsiasi disposizione del presente Contratto non valida, nulla o per qualsiasi motivo non applicabile, in toto o in parte, tale disposizione sarà riformulata più precisamente per renderla legittima e applicabile; ciò tuttavia non inficerà il Contratto e le rimanenti disposizioni del Contratto resteranno pienamente valide e in vigore nella massima misura consentita dalla legge diritto o dall'equity, conservando quanto più possibile il loro intento originale. Non varrà alcuna deroga a disposizioni o a condizioni del presente Contratto, a meno che la deroga non sia presentata per iscritto e firmata da Lei e da rappresentante autorizzato del Titolare, purché nessuna deroga a una violazione di una disposizione del presente Contratto valga come una deroga a qualsiasi violazione precedente, concorrente o successiva. La mancata insistenza da parte del Titolare nel richiedere la stretta applicazione di qualsiasi disposizione del presente Contratto o nel far valere un diritto non potrà essere interpretata quale deroga a tale disposizione o rinuncia a tale diritto.

13. **Informazioni di contatto**

    Per qualsiasi domanda relativa al presente Contratto, o se si desidera consultare per qualsiasi motivo il Titolare, si prega di contattare il nostro Servizio Clienti presso:

    Kaspersky Lab ZAO, 10 edificio 1, 1st Volokolamsky Proezd

    Mosca, 123060

    Federazione Russa

    Tel: +7-495-797-8700

    Fax: +7-495-645-7939

    E-mail: info@kaspersky.com

    Sito Web: www.kaspersky.it

INDICE

A

Aggiornamento
- da una cartella locale ... 149
- impostazioni internazionali ... 145
- in base alla pianificazione ... 147
- manuale ... 143
- modalità di esecuzione ... 146, 147
- oggetti da aggiornare ... 148
- origine degli aggiornamenti ... 144
- rollback dell'ultimo aggiornamento ... 144
- utilizzo di un server proxy ... 146

Algoritmo di funzionamento
- Anti-Hacker ... 91
- Anti-Spam ... 109
- Anti-Virus File ... 46
- Anti-Virus Posta ... 58
- Anti-Virus Web ... 68
- Difesa Proattiva ... 75

Ambito di protezione
- Anti-Virus File ... 49
- Anti-Virus Posta ... 61
- Anti-Virus Web ... 70

Analisi Attività Applicazione
- Difesa Proattiva ... 75, 76, 77

Analisi euristica
- Anti-Virus File ... 50
- Anti-Virus Posta ... 64
- Anti-Virus Web ... 71

Anti-Banner
- Anti-Spy ... 85
- elenco degli indirizzi bloccati ... 86
- elenco degli indirizzi consentiti ... 86
- esportazione / importazione degli elenchi di banner ... 87
- impostazioni avanzate ... 87

Anti-Dialer
- Anti-Spy ... 88

Anti-Hacker
- algoritmo di funzionamento ... 91
- monitor di Rete ... 104
- Sistema di rilevamento intrusioni ... 103
- statistiche sul funzionamento del componente ... 106

Anti-Spam
- addestramento ... 111
- algoritmo di funzionamento ... 109
- elenco degli indirizzi consentiti ... 119
- elenco di frasi bloccate ... 122
- elenco di frasi consentite ... 119
- elenco di indirizzi bloccati ... 121
- estensione Microsoft Office Outlook ... 123
- estensione Microsoft Outlook Express ... 125
- estensione The Bat! ... 125
- fattori di spam ... 109, 117
- filtro dei messaggi di posta sul server. ... 115
- funzioni di filtro avanzate ... 118
- impostazione dell'elenco consentiti ... 120
- livello di sensibilità ... 114
- messaggi di Microsoft Exchange Server ... 116
- potenziali fattori di spam ... 109, 117

statistiche sul funzionamento del componente 127
tecnologie di filtro 117

Anti-Spy
Anti-Banner 85
Anti-Dialer 88
statistiche sul funzionamento del componente 88

Anti-Virus File
algoritmo di funzionamento 46
ambito di protezione 49
analisi euristica 50
livello di protezione 47
modalità di scansione 52
ottimizzazione della scansione 51
reazione alle minacce 48
scansione dei file composti 51, 52
sospensione 53, 54
statistiche sul funzionamento del componente 55
tecnologia di scansione 53

Anti-Virus Posta
algoritmo di funzionamento 58
ambito di protezione 61
analisi euristica 64
filtro degli allegati 65
livello di protezione 59
reazione alle minacce 60
scansione dei file composti 64
statistiche sul funzionamento del componente 66

Anti-Virus Web
algoritmo di funzionamento 68
ambito di protezione 70
analisi euristica 71
livello di protezione 69
ottimizzazione della scansione 72
reazione alle minacce 69
statistiche sul funzionamento del componente 73

Area attendibile
applicazioni attendibili 158, 161
regole di esclusione 158, 159

Auto-difesa dell'applicazione 171

Avvio attività
scansione 131, 138, 139, 140

Avvio dell'attività
aggiornamento 143, 146, 147

Azioni da eseguire con la posta spam 123, 125

Azioni da eseguire sugli oggetti 48, 60, 69, 134

B

Backup 178, 179

C

Categorie di minacce rilevabili 158

Componenti dell'applicazione 17

D

Difesa Proattiva
algoritmo di funzionamento 75
Analisi Attività Applicazione 75, 76, 77
Registry Guard 81, 82, 83
statistiche sul funzionamento del componente 84

Disco di Ripristino 183, 184, 186

E

Elenco bloccati 86, 121, 122
Elenco consentiti 86, 119

F

Fattori di spam
Anti-Spam 109, 117
File iSwift 172
Finestra principale dell'applicazione 41
Firewall
creazione di regole per applicazioni 94
creazione di regole per i pacchetti 95
esportazione / importazione delle regole create 96
livello di protezione 92
modalità Mascheramento 102
modalità operativa 103
ottimizzazione delle regole per applicazioni e filtraggio pacchetti 97, 98, 99, 100
priorità di una regola 96
regole per applicazioni e pacchetti 93, 94, 95
regole per zone di sicurezza 100, 101, 102

I

Icona dell'area di notifica della barra delle applicazioni 39
Interfaccia dell'applicazione 39

K

Kaspersky Lab 13

L

Livello di protezione
Anti-Virus File 47
Anti-Virus Posta 59
Anti-Virus Web 69

M

Menu di scelta rapida 40
Monitor di Rete
Anti-Hacker 104

N

Notifiche 173

P

Potenziali fattori di spam 117
Protezione dagli attacchi di rete
tipi di attacchi di rete rilevabili 104

Q

Quarantena 177, 178, 179
Quarantena e backup 177, 178

R

Rapporto 176
Reazione alle minacce
Anti-Virus File 48
Anti-Virus Posta 60

Anti-Virus Web ... 69
scansione anti-virus ... 134

Recapito posta
Anti-Spam ... 115

Registry Guard
Difesa Proattiva ... 81, 82, 83

Rete
connessioni crittografate ... 180
porte monitorate ... 179

Ripristino delle impostazioni predefinite ... 55, 65, 72, 163

S

Scansione
avvio automatico dell'attività ignorata ... 139
azione da eseguire in caso di oggetto rilevato ... 134
in base alla pianificazione ... 139
livello di protezione ... 133
modalità di esecuzione ... 138, 139
ottimizzazione della scansione ... 135
scansione dei file compositi ... 136
tecnologie di scansione ... 137
tipo di oggetti da esaminare ... 135

Sistema di rilevamento intrusioni
Anti-Hacker ... 103

Statistiche sul funzionamento del componente
Anti-Hacker ... 106
Anti-Spam ... 127
Anti-Spy ... 88
Anti-Virus File ... 55
Anti-Virus Posta ... 66
Anti-Virus Web ... 73
Difesa Proattiva ... 84

T

Tecnologia avanzata di disinfezione ... 157